The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
1	**Avecto**	**DefendPoint Privilege Management**	Defendpoint provides all the tools you need to successfully manage an environment without admins. Each employee gets just the right amount of access, with permissions applied directly to approved apps, tasks and scripts - rather than to the users themselves. Standard users are highly secure, yet severely restricted. Conversely, admin users are totally free but security is compromised. By enabling all employees to work efficiently with standard user accounts, you create a much safer business environment.	https://www.avecto.com/defendpoint/privilege-management
2	**Axiomatics**	**Data Access Filter**	The Axiomatics Data Access Filter (ADAF) is an authorization service designed to intercept and modify SQL statements for the purpose of applying policy-based controls in database access scenarios. Row-level and even column-level filtering is achieved, according to policy, by modifying SQL statements with the condition clause produced by the Axiomatics Data Access Filter. It enables dynamic filtering of database content, centrally defined and managed access policies, and architecture suitable to integrate with multiple database products.	http://www.axiomatics.com/
3	**Axiomatics**	**Policy Server**	The Axiomatics Policy Server (APS) is a solution available for enterprise-wide roll out of Attribute Based Access Control (ABAC). With three different types of authorization services combined in one, it handles any and every type of access control requirements.	http://www.axiomatics.com/solutions/products/authorization-for-applications/axiomatics-policy-server.html
4	**Axiomatics**	**Reverse Query**	The Axiomatics Reverse Query (ARQ) is an authorization API which extends the capabilities of XACML-based access control. Where the Axiomatics Policy Server responds to individual authorization requests conformant with the ZACML standard, the Axiomatics Reverse Query helps automate processing of fine-grained access control for large data sets in a single batch.	http://www.axiomatics.com/component/rsfiles/preview.html?path=Data%2BSheets%252FARQ2.0_v2.pdf
5	**BDNA**	**Discover**	BDNA Discover delivers insights into the IT environment with a non-intrusive agentless technology that identifies hardware and software assets including those not covered by traditional agent-based tools. Its unique fingerprinting technology provides advanced application discovery for top vendors like Oracle, IBM, Microsoft, SAP, Adobe, and more. BDNA Discover provides complete visibility into the IT environment to drive Asset Management, SAM, License Compliance, Security and IT GRC.	http://www.bdna.com/products/discover/
6	**BDNA**	**Normalize**	BDNA Normalize is a solution that uses Technopedia, the world's largest and most up-to-date categorized repository of information about enterprise hardware and software, to aggregate and normalize raw data from more than 40 different data sources to create a single version of accurate and relevant information. Data enriched with market intelligence provides clean, accurate, and relevant data to drive effective initiatives.	http://www.bdna.com/products/normalize/
7	**BDNA**	**Technopedia**	BDNA Technopedia categorizes and aligns hardware and software products to deliver consistent, accurate, and business-relevant information. With more than 1.2 million products and 57 million data points of timely, relevant product and market intelligence about those products, Technopedia powers many IT projects within the enterprise, unifies siloed IT processes, and provides alignment with business goals.	http://www.bdna.com/products/technopedia/
8	**BeyondTrust**	**PowerBroker**	PRIVILEGED PASSWORD AND SESSION MANAGEMENT Provide secure access control, auditing, alerting and recording for any privileged account — such as local or domain shared administrator accounts; users' personal admin accounts; service, operating system, network device, database (A2DB) and application (A2A) accounts; and even SSH keys. • PRIVILEGE AND SESSION MANAGEMENT FOR UNIX & LINUX • PRIVILEGE AND SESSION MANAGEMENT FOR WINDOWS AND MAC OS X • ACTIVE DIRECTORY BRIDGING • AUDITING AND PROTECTION	https://www.beyondtrust.com/products/powerbroker/
9	**BeyondTrust**	**Retina**	Retina CS is the only vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Retina's results-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure. Over 10,000 customers worldwide rely on Retina to enable visible, measurable and actionable vulnerability management across their organizations. Retina CS Enterprise Vulnerability Management software enables you to: * Discover network, web, mobile, cloud and virtual infrastructure * Profile asset configuration and risk potential * Pinpoint vulnerabilities, malware and attacks * Analyze threat potential and return on remediation * Remediate vulnerabilities via integrated patch management (optional) * Report on vulnerabilities, compliance, benchmarks, etc. * Protect endpoints against client-side attacks	http://www.beyondtrust.com/Products/RetinaCSThreatManagementConsole/
10	**Bit9**	**Parity Suite**	The Bit9 Parity Suite 6 is an endpoint protection solution comprised of a client/server architecture that provides application whitelisting, device control, file integrity monitoring, registry protection and system protection - all within a single agent.	http://www.carbonblack.com

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
11	**Bit9**	**Security Platform**	The Bit9 Security Platform is the leader in proactive and customizable application control and endpoint threat prevention. It is trusted by more than 1,000 organizations and 25 of the Fortune 100 to secure their high-risk endpoints and servers against advanced attacks. As traditional antivirus prevention proves insufficient to protect organizations from advanced threats and malware, leading enterprises and organizations are looking to deploy next-generation application control solutions that provide complete, proactive and real-time protection for critical servers and high-risk endpoints. A policy-driven approach to endpoint security, such as the Bit9 Security Platform, can provide you with both the real-time visibility and proactive protection you need to take back control of your endpoints and servers stopping the threat at the source. How it Works: Bit9's policy-driven approach to application control combines a powerful visibility and application discovery agent with trust ratings from the Bit9 Threat Intelligence Cloud to help organizations greatly simplify and automate the set-up and administration of a secure whitelisting solution, with minimal end-user impact.	https://www.bit9.com/solutions/security-platform/
12	**BMC Software**	**Atrium**	BMC Atrium CMDB 9 provides a complete, accurate, and up-to-date view of the people, technologies, and services that make up your business and IT environments. The benefits of ITIL® CMDB span your entire IT organization—including service support, mainframe, and cloud—to give you complete control over the service lifecycle. •Increase efficiency and stability with a single source of reference for all your IT infrastructure and services. •Reduce costs by automating tasks that previously required manual intervention. •Minimize IT risks with better understanding of change dependencies. •Operate services with clear insight into all parameters. •Enable seamless integration between support and operations processes.	http://www.bmc.com/it-solutions/atrium-cmdb.html
13	**BMC Software**	**Blade Logic**	BMC BladeLogic Server Automation provides a policy-based approach for IT administrators to manage their data centers with greater speed, quality, and consistency. Broad support for all major operating systems on physical servers and leading virtualization and cloud platforms lets IT install and configure server changes with ease. Rich out-of-the-box content helps IT automate continuous compliance checks and remediation for regulatory requirements. Now IT staff can build, configure, and enforce compliance faster and more reliably. With a simplified web portal, the IT operations team can increase the server to admin ratio, gain productivity, complete audits swiftly, and quickly respond to increasing business demands.	http://documents.bmc.com/products/documents/27/36/242736/242736.pdf
14	**BMC Software**	**Client Management**	Seamlessly automate processes and effectively manage clients with BMC Client Management 12, a comprehensive set of capabilities that enable you to discover, configure, manage, and secure all of your IT end points. •Pass software audits with ease •Reduce data vulnerabilities and financial risk through automated software patching •Know what you have – confidently discover all your clients and edge devices •Intelligently manage your software entitlements – don't over deploy and don't over spend •Enjoy turnkey integration with multiple BMC service desk solutions	http://www.bmc.com/it-solutions/client-management.html
15	**BMC Software**	**Decision Support**	Welcome to the Decision Support for Server Automation (formerly BSARA-S) Community, where members who leverage BMC technology can find assistance in building solutions that solve critical business problems. BMC Software experts weigh in with commentary ranging from blogs about BSM to podcasts on CMDB trends and discovery best practices. Check out the forums for the most current discussions and practices.	https://communities.bmc.com/community/bmcdn/bmc_service_automation/reports/bsara
16	**BMC Software**	**Mobility for Remedy**	BMC Mobility apps: 1. Manage incidents, problems, assets and change. 2. Offload calls to your help desk 3. Escalate issues and respond to assigned incidents. 4. Deploy assets the minute they arrive with barcode scanners. 5. Let users to submit and track service requests. 6. Review and approve change and service requests. 7. View real-time snapshots of IT KPIs.	http://www.bmc.com/videos/solution-videos/mobility-itsm-analyst-approval.html
17	**BMC Software**	**Network Automation**	An integral part of BMC's Automation Passport and Intelligent Compliance strategies, BladeLogic Network Automation 8 keeps your business running smoothly—with no network outages or downtime—by automating network configuration, change, and compliance processes. •Cut operating costs with automation and one-click rollback. •Stop network outages by eliminating bad configuration changes. •Guarantee compliance with best practices and regulatory standards. •Extend change management initiatives to the network level.	http://www.bmc.com/it-solutions/bladelogic-network-automation.html

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
18	**BMC Software**	**Remedy IT Service**	BMC Remedy Service Management is an innovative service management platform built natively for mobile with an intuitive, beautiful, people-centric user experience that makes your whole organization more productive. Simple to use and powerful enough to manage the most advanced digital enterprises, Remedy can be delivered from the BMC cloud or your own data center. • Service desk in your pocket: Mobilize the digital workforce and take advantage of native mobile device capabilities such as touch screens, predictive text, barcode scanners, cameras, GPS, and push notifications. • Amazing user experience (UX): Smart IT is the persona-based user experience personalized to your role with context-aware insights that automatically present you with relevant content. • Intuitive self-service: Log an incident, request a service, reserve a room, download an app, or check service availability all from the convenience of a mobile app. • Engage the whole team: Embedded social and collaboration tools help you work smarter to deliver better service across the digital enterprise. • Insightful analytics: Create detailed reports with drag-and-drop simplicity and visualize them in stunning dashboards with brand new Smart Reporting.	http://www.bmc.com/it-solutions/remedy-itsm.html
19	**BMC Software**	**Server Automation**	An integral part of BMC's Automation Passport and Intelligent Compliance strategies, BladeLogic Server Automation 8 manages even the biggest change and configuration tasks simply and easily. •Cut operational costs by automating manual tasks. •Reduce service downtime with policy-based configuration management. •Manage all resources from a single platform.	http://www.bmc.com/it-solutions/bladelogic-server-automation.html
20	**CA Technologies**	**SiteMinder Web Services Security**	CA SiteMinder® Web Services Security (CA SiteMinder WSS) is a centralized, policy-based Web services security software product that helps secure access to services by inspecting the security and other content in XML messages. It enables your organization to create a centralized enterprise security service that provides authentication, authorization, federation and audit capabilities across heterogeneous IT infrastructures. This enables you to accommodate the security requirements of new application architectures at a reasonable cost.	http://www.arcserve.com/~/media/Files/ProductBriefs/1118-ca-soa-security-manager-ps-050211-2b.pdf
21	**CA Technologies**	**Advanced Authentication**	CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geo-location and user behavior profiling, as well as a wide variety of multi-factor, strong authentication credentials. This solution helps organizations provide the appropriate authentication process for each application.	http://www.ca.com/us/products/ca-advanced-authentication.html
22	**CA Technologies**	**Hytrust**	The rise of virtualization has changed almost everything about IT. With hosts being replaced by ESXi and the network by NSX with vSphere to rule them all, a lot of administrative power has been concentrated in the hypervisor but approaches to security have remained relatively stagnant until now. With HyTrust CloudControl we help harden and protect one of the top targets of hackers – the hypervisor and we help protect your infrastructure even when good credentials have fallen into the wrong hands as has been the case with a number of recent breaches including Home Depot, Target and others.	http://www.hytrust.com/products/cloudcontrol/capabilities/
23	**CA Technologies**	**Identity Management and Governance**	The CA Identity Management and Governance solution includes CA Privileged Identity Manager and CA Identity Suite. This identity management and governance solution is designed to improve business's efficiency, security and compliance by automating identity-related controls across physical, virtual and cloud environments.	http://www.ca.com/us/products/identity-management.aspx
24	**CA Technologies**	**Privileged Identity Management**	CA Privileged Identity Manager is a PIM solution that provides both broad and deep capabilities that include user access controls, shared account password management, UNIX to Active Directory authentication bridging and user activity reporting–in both physical and virtual environments.	http://www.ca.com/us/securecenter/ca-privileged-identity-manager.aspx
25	**CA Technologies**	**Shared Account Manager**	CA Shared Account Manager provides secure access to privileged accounts, manages password complexity, and helps provide accountability for privileged access through the issuance of passwords on a temporary, one-time use basis and through secure auditing of shared account accesses. CA Shared Account Manager is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard-coded passwords from scripts. Support is available for a multitude of servers, applications (including databases), and devices in physical and virtual environments.	http://www.ca.com/us/~/media/Files/DataSheets/ca-shared-account-manager.pdf
26	**CA Technologies**	**Single Sign-On (Connect & Secure)**	provide a seamless user experience by allowing your users to sign on once to access all of their applications while protecting your organization from breaches and other threats. With CA Single Sign-On, you get flexible and secure identity access management.	http://www.ca.com/us/products/connect-secure.html
27	**Centrify**	**Centrify for Applications**	Active Directory-Based Single Sign-On for Java/J2EE and Web Applications. Improve user satisfaction and streamline IT operations by giving them a single password to access all web applications running on Apache, JBoss, Tomcat, WebLogic and WebSphere.	https://www.centrify.com/app-server-plugins/web-apps/
28	**Centrify**	**Centrify Server Suite Management/Enterprise Edition**	Centrify Server Suite Management/Enterprise Edition combines bridging of Linux and UNIX systems to Active Directory with privilege management and session monitoring across Windows, Linux and UNIX systems. Identity Consolidation, Privilege Management and Audit	https://www.centrify.com/products/server-suite/
29	**Cisco Systems Inc**	**Cisco Identity Services**	Get a security policy management platform that automates and enforces context-aware security access to network resources. Cisco Identity Services Engine delivers superior user and device visibility to support enterprise mobility experiences and to control access. It shares data with integrated partner solutions to accelerate their capabilities to identify, mitigate, and remediate threats.	http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html?referring_site=smartnav

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
30	**Cisco Systems Inc**	**Cisco Prime Infrastructure**	Cisco Prime Infrastructure simplifies the management of wireless and wired networks. It offers Day 0 and 1 provisioning, as well as Day N assurance from the branch to the data center. We call it One Management. With this single view and point of control, you can reap the benefits of One Management across both network and compute.	http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html
31	**CORE Security**	**Core Impact**	CORE Impact Pro is a comprehensive, commercial-grade penetration testing product, enabling the CDAP Penetration Testers to conduct real-world assessments across a broad spectrum of risk areas, including - Social Engineering, Network Devices, Password Cracking, Web App, and Wireless.	http://www.coresecurity.com/core-impact-pro
32	**CORE Security**	**Core Insight**	CORE Insight is an enterprise-wide solution that consolidates and prioritizing vulnerabilities, identifies and eliminates attack paths to ciritcal assests, and Is also able to model threat scenarios using configurable risk criteria.	http://www.coresecurity.com/core-insight
33	**CyberArk**	**Application Identity Manager**	CyberArk Application Identity Manager, part of the CyberArk Privileged Account Security Solution, enables organizations to protect critical business systems by eliminating hard-coded credentials from application scripts, configuration files and software code, and removing SSH keys from servers where they are used by applications and scripts. Application Identity Manager offers agent and agentless deployment options to best meet the security and	http://www.cyberark.com/products/privileged-account-security-solution/application-identity-manager/
34	**CyberArk**	**Enterprise Password Vault**	CyberArk Enterprise Password Vault, a component of the CyberArk Privileged Account Security Solution, is designed to discover, secure, rotate and control access to privileged account passwords used to access systems throughout the enterprise IT environment. The solution enables organizations to understand the scope of their privileged account risks and put controls in place to mitigate those risks.	http://www.cyberark.com/products/privileged-account-security-solution/enterprise-password-vault/
35	**CyberArk**	**On-Demand Privileges Manager (OPM)**	CyberArk On-Demand Privileges Manager is a unified access control product, allowing organizations to control and monitor the commands super-users can run based on their role and task at hand. The solution reduces the usage of privileged rights within an enterprise and enforces least privilege policies for superuser rights. CyberArk On-Demand Privileges Manager replaces siloed Unix sudo command with an enterprise-ready, scalable product with unparalleled security as well as enhanced audit capabilities.	http://www.cyberark.com/products/privileged-account-security-solution/on-demand-privileges-manager/
36	**CyberArk**	**Privileged Account Security**	CyberArk is the trusted expert in privileged account security. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for on-premise, hybrid cloud and OT/SCADA environments. The CyberArk Privileged Account Security Solution is based on CyberArk Shared Technology Platform™, which combines an isolated vault server, a unified policy engine, and a discovery engine to provide scalability, reliability and unmatched security for privileged accounts.	http://www.cyberark.com/products/privileged-account-security-solution/
37	**CyberArk**	**Privileged Threat Analytics**	CyberArk Privileged Threat Analytics, part of the CyberArk Privileged Account Security Solution, is a security intelligence system that allows organizations to detect, alert, and respond to cyber attacks targeting privileged accounts. The solution is designed to identify an attack in real-time and automatically respond to stop an attacker from continuing to advance the attack. At the core of the solution, the analytics engine runs a sophisticated combination of	http://www.cyberark.com/products/privileged-account-security-solution/privileged-threat-analytics/
38	**CyberArk**	**Shared Technology Platform**	CyberArk Shared Technology Platform serves as the basis for the Privileged Account Security Solution and allows customers to deploy a single infrastructure and expand the solution to meet expanding business requirements. Seamless integration of products built on the platform provides lowest cost of ownership, and consolidated management, policy controls and reporting capabilities. The platform delivers enterprise-class security, scalability, and high availability on a single, integrated solution. Designed to integrate into any IT environment, whether on-premises or in the cloud, the platform is the foundation of the CyberArk Privileged Account Security Solution.	http://www.cyberark.com/products/cyberark-shared-technology-platform/
39	**CyberArk**	**ViewFinity**	CyberArk Viewfinity helps organizations reduce the attack surface by limiting local administrative privileges for business users, granularly controlling IT administrator privileges on Windows Servers based on role, and seamlessly elevating users' privileges when necessary and authorized. CyberArk Viewfinity also enables organizations to closely control and monitor all applications within the environment. Trusted applications may seamlessly run, malicious applications can be immediately blocked, and unknown applications can be "greylisted" and restricted, pending further analysis.	http://www.cyberark.com/products/privileged-account-security-solution/viewfinity/
40	**Damballa**	**Failsafe**	Damballa Failsafe is a solution for detecting and terminating persistent threats and targeted attacks in enterprise networks. Damballa Failsafe hunts for hidden infections and undetected threats by monitoring and analyzing egress, proxy and DNS traffic, and detecting and analyzing suspicious file downloads. By correlating suspicious network activity, Damballa Failsafe can pinpoint infected assets while profiling the severity of the threat and providing full forensics regarding threat activity and the criminal operators behind the threat.	https://www.damballa.com/products-solutions/damballa-failsafe/
41	**DB Networks**	**Adaptive Database Firewall Security Appliance**	Operating at the database tier, directly in front of the database servers, the DBN-6300 is in the perfect location to effectively analyze database traffic. It will immediately identify any undocumented databases, identify traffic to/from restricted segments, and identify advanced database attacks. When rogue SQL statements are present at the database tier it means your perimeter defenses have been breached and your application has also been exploited. The DBN-6300 stands as the final defense in your database defense-in-depth strategy.	http://www.dbnetworks.com/products/DBN-6300.htm
42	**Dell**	**Asset Manager**	The Dell Asset Manager is a solution for managing software and hardware assets. Through a single console, it allows users to discover and track asset inventory and license agreements. Plus, users can automatically generate usage reports to correlate actual software purchases and entitlements. Asset Manager also goes beyond simply scanning and identifying software. It tracks usage through metering and quickly identifies whether software is being underutilized, sitting idle or if the appropriate number of licenses have not been purchased.	http://software.dell.com/products/asset-manager/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
43	Dell	ChangeAuditor	The Dell Change Auditor is a solution that gives complete, real-time change auditing, in-depth forensics and comprehensive reporting on all key configuration, user and administrator changes for Active Directory, ADLDS, AD Queries, Exchange, SharePoint, Lync, VMware, NetApp, Windows File Servers, EMC, and SQL Server. Change Auditor also tracks detailed user activity for web storage and services, logon and authentication activity and other key services across enterprises. A central console eliminates the need and complexity for multiple IT audit solutions.	http://software.dell.com/products/change-auditor/
44	Dell	Changebase	Dell ChangeBase is a product that allows for automation of application compatability testing, application remediation, application packaging, and application virtualization to reduce the risk of migrating while ensuring application readiness.	http://software.dell.com/products/changebase/
45	Dell	Identity Manager	The Dell One Identity Manager is a solution that allows for unification of security policies, meets compliance needs and achieves governance while improving business agility today and in the future with a modular and scalable Identity and Access Management solution. It governs identities, secures data and drives identify and access management by business needs, not IT capabilities.	http://software.dell.com/products/identity-manager/
46	Dell	Kace	Dell KACE products deliver comprehensive systems and device management from initial deployment through maintenance, security and support, using an all-in-one appliance architecture that is easy to use, fast to deploy and delivers rapid return on investment . Combined with Dell Enterprise Mobility Management and Dell Desktop Authority Management Suite, KACE products enable you to manage mobile devices, gain centralized and granular control of your end-user work environment, and automate the "anypoint" management of your entire connected IT infrastructure.	http://software.dell.com/kace/
47	Dell	One Cloud Access Manager	The Dell Cloud Access Manager (CAM) is a web-access management solution that offers secure and unified access to all internal and cloud-based web applications while simultaneously enhancing security and IT efficiency. CAM enables: adaptive security, scalable just-in-time cloud provisioning, secure identity federation, simplified access control and auditing, and single sign-on.	http://software.dell.com/products/cloud-access-manager/
48	Dell	Password Manager	The Dell Password Manager is a solution that provides a self-service that allows end-users to reset forgotten passwords and unlock their accounts. It permits administrators to implement stronger password policies while reducing the help-desk workload.	http://software.dell.com/documents/password-manager-datasheet-19909.pdf
49	Dell	Privilege Management	Control and audit administrative access through secure, automated, policy-based workflows with Dell One Identity solutions. These solutions provide capabilities for granting access, granular delegation of “superuser” rights, session recording and key stroke logging of activity, and governance over privileged access and accounts. The results are enhanced security and compliance with more efficient “superuser” access administering, tracking and auditing.	http://software.dell.com/solutions/privileged-management/
50	Dell	Privileged Access Suite for Unix	The Dell Privileged Access Suite for Unix is a solution that consolidates and unifies Unix, Linux, and Mac OS X identities. It assigns individual accountability and allows centralized reporting, giving you and your users access to the systems. Privileged Access Suite for Unix also provides least privilege capabilities, ensuring that administrators can only access what they need in order to perform their jobs. The all-in-one suite for Unix security combines Active Directory bridge and root-delegation solutions under a unified console. This gives organizations centralized visibility and more efficient administration of access rights and identities across their entire Unix environment.	http://software.dell.com/products/privileged-access-suite-for-unix/
51	Dell	Privileged Session Management	Privileged Session Manager enables you to issue privileged access, while meeting auditing and compliance requirements. Privileged Session Manager is deployed on a secure, hardened appliance and allows you to grant access to administrators, remote vendors and high-risk users for a specific period or session, with full recording and replay for auditing and compliance. It gives you a single point of control to authorize connections, view active connections and limit access to specific commands and resources, as well as record all activity, alert if connections exceed pre-set time limits, and terminate connections.	http://software.dell.com/products/privileged-session-manager/
52	Dell	Quest ActiveRoles	Quest ActiveRoles is a solution that allows automated tools to efficiently manage users and groups, as well as Active Directory delegation, ActiveRoles Server overcome Active Directory’s native limitations. With ActiveRoles Server, users can eliminate unregulated access to resources while protecting critical Active Directory data and automatically create user and group accounts for secure management in AD and AD-joined systems.	http://software.dell.com/products/activeroles-server/
53	Dell	Quest Enterprise Single Sign-On	Quest Enterprise Single Sign-On is a solution that enables organizations to streamline both end-user management and enterprise-wide administration of single sign-on (SSO). It bases application and system user logins on existing Active Directory identities, so there’s no infrastructure to manage.	http://software.dell.com/products/esso/
54	Dell	QuickConnect	The Dell One Quick Connect is a solution that can completely automate the process of identity data synchronization between the data systems used in an enterprise environment. Quick Connect increases the data management efficiency by allowing users to automate the provision, deprovision, and update operations between the data systems they use. The use of scripting capabilities provides a flexible way to automate day-to-day administration tasks and integrate the administration of managed data systems with other business processes. By automating regular synchronization tasks, Quick Connect allows administrators to concentrate on strategic issues, such as planning the directory, increasing enterprise security, and supporting business-critical applications.	https://support.software.dell.com/one-identity-quick-connect-sync-engine/5.4
55	Dell	Total Privileged Access Manager	Dell Total Privileged Access Management (TPAM) 2.5 – formerly Quest Total Privileged Access Management, is a robust collection of integrated modular technologies designed specifically to meet the complex and growing compliance and security requirements associated with privileged identity management and privileged access control. The TPAM Suite provides organizations the flexibility to solve the critical issues associated with compliant privileged control in a modular fashion as needed on an integrated appliance. The TPAM Suite modules include Privileged Password Management (PPM), Privileged Session Management (PSM), Application Password Management (APM), and Privileged Command Management (PCM).	http://software.dell.com/solutions/privileged-management/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
56	**Dell**	**Virtual Directory Server**	The Dell Virtual Directory Server is a middleware application solution that abstracts back-end data from client applications. Virtual Directory Server allows users to easily integrate new applications into their existing identity infrastructure without having to alter directory information. That means data stays put and in the same format. Run Virtual Directory Server in environments where a variety of operating systems are used. This solution has been ported to all major platforms and optimized. Improve overall performance through load balancing and search caching using a single granular security policy for all back-end repositories.	http://software.dell.com/products/virtual-directory-server/
57	**eIQ**	**SecureVue**	SecureVue helps Information Assurance and Cyber Security Managers automate a number of the requirements outlined in various federal regulations including 800-53, 8500.2, CNSSI, and the Risk Management Framework. The core SecureVue capabilities include: • Audit Log Management & SIEM • Continuous STIG & USGCB Compliance Monitoring • Risk Management Framework (RMF) Compliance • STIG Assessments for IT Auditors • Cyber Analytics	http://www.eiqnetworks.com/Federal/solutions.php
58	**Endgame**	**Global Crawl Data**	Global Crawl Data - Worldwide infrastructure data yearly subscription	https://www.endgame.com/our-platform
59	**Endgame**	**Lightstorm**	Lightstorm - Cyber reconnaissance and analysis application platform	https://www.endgame.com/our-platform
60	**Endgame**	**Touchpoint**	Torchpoint - Command and control and situational awareness application platform	https://www.endgame.com/our-platform
61	**ForeScout**	**ForeScout CounterACT**	ForeScout CounterACT is a platform that provides continuous security monitoring and mitigation. It allows IT organizations to efficiently address numerous access, endpoint compliance and threat management challenges even within today's complex, dynamic and expansive enterprise networks. Taking advantage of next-gen network access control (NAC) capabilities, CounterACT delivers both real-time intelligence and policy-based control to preempt threats and remediate problems while preserving business productivity.	http://www.forescout.com/product/counteract/
62	**ForgeRock**	**Open Source Platform to include: Common Services, Access Management, User-Managed Access, Identity Management Identity Gateway, Directory Services**	A ForgeRock subscription gives you full access to enterprise-ready products developed by our world-class engineering team. Our bundled offering includes a software license, global support, and legal indemnification, giving you the power, protection, and assurance you need to successfully deploy best-of-breed identity and access management solutions.	https://www.forgerock.com/platform/
63	**Hewlett-Packard**	**Application Defender**	HPE's runtime application self-protection can help you stop security threats that no one else can even see by protecting production applications from the inside. It's application security simplified.	http://www8.hp.com/us/en/software-solutions/appdefender-application-self-protection/
64	**Hewlett-Packard**	**ArcSight**	ArcSight Enterprise Security Manager (ESM) is a security data correlation engine used to provide enterprise situational awareness. It can analyze and correlate a large number of event types (e.g., login, logoff, file access, database query, etc.) to allow prioritization of security risks and compliance violations. The correlation engine can identify incidents to be presented through real-time dashboards, notifications, or reports. It can model IP addresses/network zones, systems and devices, users, employees, customers and partners. It can apply techniques such as pattern recognition and behavioral analysis. It has a built-in workflow engine to manage incidents. ESM Console provides a nice GUI. Supports analysis through correlation of every event that occurs across the organization. The powerful correlation engine can sift through millions of log records to find the critical incidents that matter. These incidents are then presented through real-time dashboards, notifications, or reports to the security administrator.	http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/index.html
65	**Hewlett-Packard**	**ArcSight Adoption Readiness Tool**	HP Software's Adoption Readiness Tool is the perfect marriage of content created by HP Software Subject Matter Experts and the content development tools that you can use to create and customize content to meet the needs of your environment. Choose to deliver the pre-designed core content (i.e. Asset Manager), or customize your own and roll out across your entire organization – resulting in a comprehensive documentation, training and support strategy.	http://h20546.www2.hp.com/main/US/news.cfm?NewsID=179&jumpid=va_R11374_us/en/large/eb/software
66	**Hewlett-Packard**	**Asset Manager Enterprise Suite**	HP Asset Manager delivers out-of-the-box, real-time federation with HP Universal Configuration Management Database (UCMDB). This integration results in one of the few systems to automate the entire IT Service Management process without requiring a monolithic repository. Federation reduces data redundancy and improves transaction performance—so that relevant data resides within its respective business domain, yet is available across the business infrastructure. In addition, discovered services or mapped views of component configuration items can be correlated to their physical assets, enabling IT to rationalize the fiscal cost of delivering these business services to customers. HP Asset Manager offers a huge benefit for organizations looking to reduce costs of maintaining ITIL-aligned integrations, optimize transaction performance, and share critical data across the business infrastructure.	http://www8.hp.com/us/en/software-solutions/asset-management-software/index.html
67	**Hewlett-Packard**	**Atalla**	HP Atalla is a data-centric security and encryption solution that neutralizes breach impact by securing sensitive data at rest, in use and in motion. It provides advanced encryption, tokenization and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission critical transactions, storage and big data platforms.	http://www8.hp.com/us/en/software-solutions/data-security-encryption/index.html
68	**Hewlett-Packard**	**BSA Subscription**	HP Business Service Automation Essentials suite. Improve security and compliance; collaborate with the HP Business Service Automation community	http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA1-0625ENW.pdf

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
69	**Hewlett-Packard**	**Client Automation Enterprise**	Desired-State across Physical, Mobile, Virtual Devices. Accelerite Endpoint Management (formerly Radia Client Automation) from Persistent Systems enforces policy while it monitors, alerts, automates remediation, and reports on hardware, applications, and OS status. A reliable, desired-state manageability solution for highly complex and ever-changing enterprise client infrastructure, it helps you automate client management across physical or virtual clients—from assessment to deployment, migration, and retirement.	http://www8.hp.com/us/en/software-solutions/client-automation-management-software/
70	**Hewlett-Packard**	**Database Security Assessment**	HP Security Assessment Services will assist you in identifying the combination of technical, resource, and process controls that your company can use to manage security risks. Conducted by an HP security consultant, these in-depth assessments identify the strengths and weaknesses of your current security posture as well as vulnerabilities to security threats.	http://www8.hp.com/h20195/v2/GetPDF.aspx/5982-4155ENN.pdf
71	**Hewlett-Packard**	**Enterprise Secure Key Manager**	Enterprise Secure Key Manager (ESKM). Key management solution to protect your data and reputation, and comply with industry regulations.	http://www8.hp.com/us/en/software-solutions/eskm-enterprise-secure-key-management/
72	**Hewlett-Packard**	**Fortify**	HP Fortify is a software security solution that provides integrated, holistic, approach to application security for agile development. It allows the systematically test and scan applications that are developed in-house, by a thrid-party, open source, or off-the-shelf.	http://www8.hp.com/us/en/software-solutions/application-security/index.html
73	**Hewlett-Packard**	**HP TippingPoint**	The HP TippingPoint Threat Protection System (TPS) offers comprehensive threat protection against advanced and evasive targeted attacks with high accuracy. Using a combination of technologies including, but not limited to, deep packet inspection, threat reputation and advanced malware analysis, the TPS provides enterprises a proactive approach to security that includes comprehensive contextual awareness, in-depth analysis of network traffic, and the visibility and agility necessary to keep pace with today's dynamic enterprise networks.	http://www8.hp.com/us/en/software-solutions/network-security/index.html
74	**Hewlett-Packard**	**Network Automation Tool**	HP Network Automation software automates the complete operational lifecycle of network devices from provisioning to policy-based change management, compliance, and security administration. When combined with HP Network Node Manager i (NNMi) software, you get an integrated solution that unifies network fault, availability, and performance with change, configuration, compliance, and automated diagnostics. Network Automation is one component of the HP network management solution which provides a holistic, automated approach across the network management domain.	http://www8.hp.com/us/en/software-solutions/network-automation/
75	**Hewlett-Packard**	**Network Node Manager**	Network management software that unifies fault, availability, and performance monitoring to help you improve network uptime and performance, and increase responsiveness to business needs.	http://www8.hp.com/us/en/software-solutions/network-node-manager-i-network-management-software/
76	**Hewlett-Packard**	**Network Security Processor**	HPE Atalla Ax160 Network Security Processors (NSPs) provide unrivaled protection for Triple Data Encryption Standard (3DES) and other ryptographic keys when safeguarding value-based transactions. They are designed as the hardware security module complement to the Atalla Key Block, an industry-leading advanced key management solution.	http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-6651ENW.pdf
77	**Hewlett-Packard**	**Next Generation FW**	TippingPoint Next-Generation Firewall Features. Use more than 9,000 security filters that address zero-day attacks and known vulnerabilities.	http://www8.hp.com/us/en/software-solutions/ngfw-next-generation-firewall/
78	**Hewlett-Packard**	**Next Generation IPS**	Next-Generation Intrusion Prevention System - IPS. In-line, real-time Intrusion Prevention System (IPS) to defend critical data and applications from advanced attacks without affecting performance and productivity.	http://www8.hp.com/us/en/software-solutions/ngips-intrusion-prevention-system/
79	**Hewlett-Packard**	**Operations Orchestration**	Operations Orchestration. IT process automation and run book software that improves service quality and customer satisfaction, and lowers costs by eliminating latency between silos, increasing first time right rate, enforcing standards, and delivering reports for ROI, audits and more.	http://www8.hp.com/us/en/software-solutions/operations-orchestration-it-process-automation/
80	**Hewlett-Packard**	**SaaS Application Security Center**	Software as a Service (SaaS). HPE SaaS Solutions are engineered to be a core part of modern enterprise's IT infrastructure by providing a flexible, cost effective, and efficient way to purchase, deploy, and manage software.	http://www8.hp.com/us/en/software-solutions/saas-software-as-a-service/
81	**Hewlett-Packard**	**Server Automation**	Server Automation. Increase speed and reduce cost by automating server provisioning, patching and compliance across physical and virtual environments.	http://www8.hp.com/us/en/software-solutions/server-automation-software/
82	**Hewlett-Packard**	**Service Delivery Platform**	Service Delivery Platform (SDP) is HP's blueprint for developing, provisioning, and deploying standards-based end-user across multiple network types–fixed, mobile, and broadband–and generations-2G/2.5G/3G/IMS.	http://h71019.www7.hp.com/enterprise/downloads/SDP_SolutionBrief.PDF
83	**Hewlett-Packard**	**Service Manager**	Service Desk. Service desk & help desk management software that quickly and efficiently handles change and incident management while bringing together a broad range of ITSM capabilities, Big Data and social collaboration to enable your workforce with connected intelligence.	http://www8.hp.com/us/en/software-solutions/service-desk/
84	**Hewlett-Packard**	**Software Security Center**	Software Security Center. HP Fortify Software Security Center is a centralized management repository providing visibility to an organizations entire application security program, helping to resolve security vulnerabilities across your software portfolio.	http://www8.hp.com/us/en/software-solutions/software-security-assurance-sdlc/
85	**Hewlett-Packard**	**SYMC Endpoint Protection**	Symantec – HP Agility Alliance Partnership Join Forces to Offer End-to-End Security Management for Enterprise Customers	http://www8.hp.com/us/en/business-services/it-services.html?compURI=1080819
86	**Hewlett-Packard**	**Threat Assessment**	HP Comprehensive Applications Threat Analysis Service does just that. We can analyze applications early in the lifecycle to identify vulnerabilities and recommend changes where you realize the most value—before coding begins. HP Comprehensive Applications Threat Analysis Service drives down the cost of making applications secure by finding threats early to avoid rework and can avoid many more vulnerabilities than testing alone.	http://www8.hp.com/us/en/business-solutions/solution.html?compURI=1087508

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
87	**Hewlett-Packard**	**UCMDB**	This comprehensive set of CMDB tools collects, stores, manages, updates, and presents data about software and infrastructure services configuration so you can lower costs and mitigate risk. You are in a carousel. To navigate forward use right or up arrows. To navigate back use left or down arrows. HP Universal Configuration Management Database (CMDB) Data Sheet. Universal Configuration Management Database (UCMDB)	http://www8.hp.com/us/en/software-solutions/configuration-management-system-database/
88	**Hewlett-Packard**	**Universal Discovery Inventory**	http://community.hpe.com/t5/Business-Service-Management/Introducing-HP-Universal-Discovery-10/ba-p/5736029	http://community.hpe.com/t5/Business-Service-Management/Introducing-HP-Universal-Discovery-10/ba-p/57
89	**Hewlett-Packard**	**User Behavior Analytics**	UBA gives enterprises visibility into their users, making it much easier for them to gain information on behavior patterns to help mitigate threats. It helps detect and investigate malicious user behavior, insider threat and account misuse. Therefore, it enables organizations to detect breaches before significant damage occurs by finding the adversary faster.	http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA5-8223ENW
90	**Hewlett-Packard**	**WebInspect**	HP WebInspect is the industry-leading Web application security assessment solution designed to thoroughly analyze today's complex Web applications and Web services for security vulnerabilities. With broad technology cover and application runtime visibility through the HP WebInspect Agent, HP WebInspect provides the broadest dynamic application security testing coverage and detects new types of vulnerabilities that often go undetected by black-box security testing technologies.	http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-5363ENW.pdf
91	**HyTrust**	**CloudControl**	The rise of virtualization has changed almost everything about IT. With hosts being replaced by ESXi and the network by NSX with vSphere to rule them all, a lot of administrative power has been concentrated in the hypervisor but approaches to security have remained relatively stagnant until now. With HyTrust CloudControl we help harden and protect one of the top targets of hackers – the hypervisor and we help protect your infrastructure even when good credentials have fallen into the wrong hands as has been the case with a number of recent breaches including Home Depot, Target and others.	http://www.hytrust.com/products/cloudcontrol/capabilities/
92	**IBM**	**COGNOS Business Intelligence**	IBM Cognos Business Intelligence turns data into past, present and future views of your organization's operations and performance so your decision makers can capitalize on opportunities and minimize risks. You can use these views to understand the immediate and downstream effects of decisions that span potentially complex interrelated factors. Consistent snapshots of business performance are provided in enterprise-class reports and independently assembled dashboards based on trusted information. As a result, non-technical and technical business intelligence (BI) users and IT alike can respond quickly to rapidly changing business needs. Cognos Business Intelligence provides capabilities designed to provide: * Faster time to answers about business from highly visual, interactive dashboards without lengthy deployment delays * Easier access to game-changing insights with interactive data visualizations that enable you to more easily identify performance issues and apply corrective actions * Smarter decisions that drive a better outcome from snapshots of business performance * Trusted data for more consistent decisions without data drift or duplication * Flexible cloud and on-premise deployment options that can grow as your business grows and help you meet diverse organizational requirements	http://www-03.ibm.com/software/products/en/business-intelligence
93	**IBM**	**Decision Center**	IBM® Decision Center provides a repository and management capabilities for line-of-business professionals to participate in the definition and governance of rules-based decision logic. Business and IT functions can work collaboratively to align the organization in the implementation of automated decisions. IBM Decision Center accelerates the maintenance lifecycle and helps you evolve decision logic based on new external and internal requirements.	http://www-03.ibm.com/software/products/en/decision-center
94	**IBM**	**Endpoint Manager**	IBM BigFix responds to malicious cyber attacks and unintentional user induced errors using real-time visibility and control of your endpoints – along with automated quarantine and remediation capabilities.	http://www-03.ibm.com/software/products/en/category/unified-endpoint-management
95	**IBM**	**Federated Identity Manager**	The IBM Tivoli Federated Identity Manager provides web and federated single sign-on (SSO) to users throughout multiple applications. It uses federated SSO for security-rich information sharing for private, public and hybrid cloud deployments. Now you can enable security-rich business collaboration in the cloud.	http://www-03.ibm.com/software/products/en/federated-identity-mgr
96	**IBM**	**InfoSphere**	The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, big data and information governance. The platform provides an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster. Core capabilities include * Information Integration and governance * Data Refinement * Big Data * Data Warehousing	http://www-01.ibm.com/software/data/infosphere/
97	**IBM**	**Integration Designer**	IBM Integration Designer is an Eclipse-based software development tool that renders your current IT assets into service components for reuse in service-oriented architecture (SOA) solutions. IBM Integration Designer (previously known as WebSphere Integration Developer) features a visual drag-and-drop programming and test environment and integrates tightly with WebSphere Enterprise Service Bus (ESB), WebSphere DataPower, and other WebSphere adapters and business process management (BPM) platforms.	http://www-03.ibm.com/software/products/en/integration-designer
98	**IBM**	**MaaS360**	BM MaaS360 is an enterprise mobility management solution that secures and manages mobile devices, apps and content.	https://www.ibm.com/marketplace/cloud/mobile-device-management/us/en-us

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
99	IBM	Privileged Identity Manager	IBM® Security Privileged Identity Manager protects, automates and audits the use of privileged identities to help thwart insider threats and improve security across the extended enterprise, including cloud environments. A virtual appliance option and redesigned user interface makes IBM Security Privileged Identity Manager simple to install and manage.	http://www-03.ibm.com/software/products/en/pim
100	IBM	Process Center Designer and Server	The Process Center includes a repository for all processes, services, and other assets created in the IBM® Business Process Manager authoring environments, Process Designer and Integration Designer. Process Designer is available in all editions of the product. IBM Business Process Manager Advanced also offers case management and Integration Designer with its associated editors and adapters.	https://www-01.ibm.com/support/knowledgecenter/SSFPJS_8.5.5/com.ibm.wbpm.main.doc/topics/cbpm_pro
101	IBM	Qradar Incident Forensics	The IBM Security QRadar Incident Forensics allows you to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents. It reduces the time it takes security teams to investigate offense records, in many cases from days to hours—or even minutes. It can also help you remediate a network security breach and prevent it from happening again. IBM Security QRadar Incident Forensics offers an optional IBM Security QRadar Packet Capture appliance to store and manage data used by IBM Security QRadar Incident Forensics if no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.	http://www-03.ibm.com/software/products/en/qradar-incident-forensics
102	IBM	Qradar SIEM	The IBM Security QRadar SIEM consolidates log source event data from thousands of devices endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. As an option, this software incorporates IBM Security X-Force Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM Security QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.	http://www-03.ibm.com/software/products/en/qradar-siem
103	IBM	Qradar Vulnerability Manager	The IBM Security QRadar Vulnerability Manager proactively discovers network device and application security vulnerabilities, adds context and supports the prioritization of remediation and mitigation activities. It is fully integrated with the IBM QRadar Security Intelligence Platform, and enriches the results of both scheduled and dynamic vulnerability scans with network asset information, security configurations, flow data, logs and threat intelligence to manage vulnerabilities and achieve compliance. IBM Security QRadar Vulnerability Manager helps develop an optimized plan for addressing security exposures. Unlike stand-alone tools, the solution integrates vulnerability information to help security teams gain the visibility they need to work more efficiently and reduce costs. The IBM Security QRadar Vulnerability Manager is part of the IBM Security QRadar SIEM architecture. It can be quickly activated with a licensing key and requires no new hardware or software appliances.	http://www-03.ibm.com/software/products/en/qradar-vulnerability-manager
104	IBM	Security Access Manager	IBM Security Identity and Access Manager provides: * Automated user lifecycle management: Optimizes productivity and reduces cost of managing and revoking user profiles, credentials and access rights throughout the user lifecycle. * Security-rich access to web applications and data: Safeguards access to online applications and data spread across the extended enterprise. * Security compliance: Provides audit trail collection, correlation and reporting. * Convenient single sign-on (SSO): Simplifies secure access to various web-based applications and services.	http://www-03.ibm.com/software/products/en/identity-access-manager
105	IBM	Security Directory Integrator	The IBM Security Directory Integrator helps build an authoritative data infrastructure by integrating data from directories, databases, collaborative systems, applications and other data sources.	http://www-03.ibm.com/software/products/en/directoryintegrator
106	IBM	Security Identity Manager for Role Management	The IBM Security Identity Manager is a comprehensive, policy-based identity and access assurance solution with role management capabilities that helps automate the provisioning, managing and terminating of user roles, identities and access rights across the extended enterprise.	http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=TID10294USEN
107	IBM	Security Key Lifecycle Manager	The IBM Security Key Lifecycle Manager—formerly Tivoli Key Lifecycle Manager—centralizes, simplifies and automates the encryption and key management process to help minimize risk and reduce operational costs. It offers robust key storage, serving and lifecycle management for IBM and non-IBM storage devices. IBM Security Key Lifecycle Manager helps meet regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA). It supports the OASIS Key Management Interoperability Protocol (KMIP) standard.	http://www-03.ibm.com/software/products/en/key-lifecycle-manager
108	IBM	Security Policy Manager	The IBM Tivoli Security Policy Manager externalizes security policies from applications, enabling you to centralize and simplify application entitlement and fine-grained data access control. The result is strengthened access control for applications and services that improves regulatory compliance and governance across the enterprise.	http://www-03.ibm.com/software/products/en/security-policy-manager
109	IBM	X-Force	These security professionals monitor and analyze security issues from a variety of sources, including its database of more than 96,000 computer security vulnerabilities, its global web crawler with over 25B catalogued web pages and URLS, international spam collectors, and millions of malware samples collected daily. The X-Force produces many thought leadership assets including the IBM X-Force Threat Intelligence Report to help customers, fellow researchers and the public at large better understand the latest security risks, and stay ahead of emerging threats.	http://www-03.ibm.com/security/xforce/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
110	**Imanami**	**GroupID Automate, Password Center, Self-Service, Synchronize**	Imanami's GroupID revolutionizes how IT manages Active Directory groups. Your Exchange distribution lists and AD security groups will never again be out of date. Active Directory groups are essential to any organization. Accurate distribution lists improve productivity; accurate AD security groups improve security. An estimated 70% of all organizations don't have a reliable Active Directory group management solution. Without a way to automate AD group membership, an organization's security groups don't grant the correct access and distribution lists don't go to the correct users. GroupID solves these AD group management problems. AD groups are automated and managed dynamically. Users have the option of web based AD self-service to manage their own groups and group memberships… and IT has control over the process.	http://www.imanami.com/groupid/overview/
111	**Infoblox**	**DNS Firewall**	Protection from APTs and malware communicating with C&Cs and botnets. Infoblox leverages our market-leading DNS technologies into the industry's first true DNS-based network security solution.	https://www.infoblox.com/products/secure-dns/dns-firewall
112	**Infoblox**	**NetMRI**	NetMRI provides automatic network discovery, switch port management, network change automation, and continuous security policy and configuration compliance management for multi-vendor routers, switches, and other layer-2 and layer-3 network devices. NetMRI is the only platform that supports traditional and virtual network constructs (such as VRF) for multi-vendor network automation.	https://www.infoblox.com/products/network-automation/netmri
113	**Infoblox**	**Trinzic**	Infoblox Trinzic DDI is the world's leading appliance-based, integrated DNS, DHCP and IP Address Management (DDI) product.	https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-datasheet-trinzic-ddi-overview.pdf
114	**Infor**	**Infor Approva**	Infor Approva Continuous Monitoring enables you to execute repeatable and reliable processes to meet the control aspects of Governance, Risk and Compliance (GRC) requirements for your organization. Because the product provides a holistic view of data across multiple business environments, you get the visibility you need to minimize your organization's risk of noncompliance, security and governance breaches. Infor Approva CM is the only solution with out-of-the-box content that monitors and correlates all four control types for multiple applications and all major business processes. * Transaction monitoring across business application/across platforms * Verifying the integrity of Master Data * Testing and managing user access to applications against approved entitlements * Verifying legitimate application and process configurations	http://www.infor.com/product-summary/fms/approva-continuous-monitoring/
115	**Infor**	**Infor HCM**	Infor Workforce Management is a comprehensive solution that aligns labor management with corporate strategy. Integrated modules address forecasting and budgeting, scheduling, time and attendance, performance management, and compliance, streamlining processes to increase efficiency while encouraging employees to focus on activities that generate more value.	http://www.infor.com/product-summary/hcm/workforcemanagement/
116	**Infor**	**Infor Technology**	Infor 10x, the latest release of Infor's proven business applications, marries modern technologies with traditional applications, so you get the best of both worlds—solutions backed by decades of practical application that are continually enhanced with the latest technological innovations. Infor 10x delivers major advancements across all of Infor's core product lines, allowing you to maximize your investments in existing technologies and take advantage of innovative new solutions without committing to complex integrations and endless implementations. You also get access to innovative, forward-thinking solutions capable of transforming the way you work.	http://www.infor.com/solutions/technology/
117	**Informatica**	**ActiveVOS**	ActiveVOS is a service oriented process automation platform specifically designed to address the needs of the members of IT project teams – architects, developers and project managers. In ActiveVOS, you can quickly create BPMN2.0 compliant process models that seamlessly integrate people, processes and systems, increasing the efficiency and visibility of your business. When deployed, ActiveVOS executes BPMN models directly on a high-performance BPEL engine that runs on any standards-based Java Enterprise Edition server, including Oracle® Web Logic Server®, IBM® WebSphere® Application Server, JBoss® Application Server or Apache Tomcat. ActiveVOS offers complete compatibility and rigorous support for open standards, enabling process automation to become a generalized service across the enterprise. In this way, process applications never become an "island" of processing.	http://www.activevos.com/
118	**Informatica**	**B2B Data Transformation**	Extract and Utilize Data from Any File, Document, or Message	https://www.informatica.com/content/dam/informatica-com/global/amer/us/collateral/data-sheet/b2b-data-
119	**Informatica**	**Big Data Governance Edition**	Ingest, process, clean, govern, and secure big data so organizations can repeatably deliver trusted information for analytics.	https://www.informatica.com/products/big-data/big-data-edition.html#fbid=ipvbK6EDcSj
120	**Informatica**	**Big Data Relatinship Mgmt**	Ensure the success of big data analytics projects by uncovering accurate relationships among connected data.	https://www.informatica.com/products/big-data/big-data-relationship-manager.html#fbid=ipvbK6EDcSj
121	**Informatica**	**Informatica Data Security**	Prevent unauthorized users from accessing sensitive information with real-time data de-identification and de-sensitization.	https://www.informatica.com/products/data-security/data-masking/dynamic-data-masking.html#fbid=ipvbK6
122	**Informatica**	**Informatica Identity Resolution**	Search systems and databases to discover hidden connections between people.	https://www.informatica.com/products/master-data-management/identity-resolution.html#fbid=ipvbK6EDcSj
123	**Informatica**	**Informatica Master Data Management (MDM)**	Master data management (MDM) is a methodology that identifies the most critical information within an organization—and creates a single source of its truth to power business processes. MDM involves a number of technology solutions, including data integration, data quality, and business process management (BPM). It delivers a single view of the data, a 360-degree view of relationships, and a complete view of all interactions.	https://www.informatica.com/products/master-data-management.html - fbid=UHBQ0MqXFQD

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
124	**Informatica**	**Informatica PowerCenter**	The Informatica PowerCenter is a solution that uses an automated, repeatable, scalable, and auditable approach to test and monitor critical data integration processes. It also provides an "early-warning system" that proactively monitors, alerts, and enforces both the enforcement of development best practices as well as PowerCenter operations.	https://www.informatica.com/products/data-integration/powercenter.html - fbid=UHBQ0MqXFQD
125	**Informatica**	**Informatica PowerExchange**	Cost-effectively, quickly, and easily access and integrate all data with out-of-the-box, high-performance connectors that enable your IT organization to access all enterprise data sources without having to develop custom data access programs.	https://www.informatica.com/products/data-integration/connectors-powerexchange.html - fbid=OnzJD47jTg0
126	**Informatica**	**Informatica Rule Point**	RulePoint complex event processing software provides proactive monitoring and operational intelligence by delivering real-time alerts and insight into pertinent information, enabling you to operate smarter, faster, more efficiently, and more competitively. Its real-time alerts are based on sets of conditions defined by business users. RulePoint key features include the following: •Supports users' various skill modes — with templates and wizards to advanced features — so operational intelligence can be delivered regardless of skill. •Accelerates roll-out of templates to business users in existing web portals, increasing the efficiency of operational intelligence. •Monitors diverse and disparate data or event sources, including event streams, sensors, communications systems, message queues, web services, RSS feeds, databases, and flat files, for robust operational intelligence. Natively processes both real-time and batch data. •Leverages custom/proprietary data sources and functions and easily integrates into third-party user interfaces, portals, and applications. •Pushes alerts about critical threats and opportunities to a web-based persistent communications channel, email, and any other destination.	https://www.informatica.com/products/data-integration/real-time-integration/rulepoint-complex-event-proce
127	**Informatica**	**Informatica VIBE Data Stream**	Informatica Vibe Data Stream for Machine Data (VDS) helps manage many small pieces of data as they flow in at high rates and accumulate quickly into large volumes. Vibe Data Stream is purpose-built for efficiently collecting all forms of streaming data and delivering it directly to both real-time and batch processing technologies A distributed, scalable system, Vibe Data Stream uses Informatica's proven high-performance brokerless messaging technology to greatly simplify streaming data collection. Features include: Lightweight agents for an ecosystem of sources and targets, brokerless messaging transport using a publish/subscribe, model, flexibility to connect sources and targets in numerous patterns, high-performance delivery direct to targets over LAN/WAN, and simplified configuration, deployment, administration, and monitoring.	https://www.informatica.com/products/data-integration/real-time-integration/vibe-data-stream.html - fbid=U
128	**Informatica**	**Ultra Messaging**	Enjoy the fastest messaging on the market with sub-100-nanosecond latency, 24x7 reliability, and extremely high throughput.	https://www.informatica.com/products/data-integration/real-time-integration/ultra-messaging.html#fbid=ipvb
129	**Intec Billing (CSG Invotas)**	**Invotas Security Orchestrator (ISO)**	Invotas Security Orchestrator (ISO), is an Automated Threat Response platform that integrates enterprise security management into a single console, giving you the ability to unify your defenses, orchestrate your response, and automate your counterattacks. Using the tools and technology you already own, and the procedures and policy you've already created, Invotas Security Orchestrator brings all of it together, improving your SOC's incident reaction time, and helping you take back the initiative.	http://invotas.csgi.com/invotas-security-orchestrator
130	**Juniper**	**Junos Secure Analytics (JSA)**	Secure Analytics- Monitor Security Threats. Market-leading security information and event management (SIEM) that consolidates large volumes of event data from thousands of Juniper and non-Juniper devices, endpoints, and applications in near real time.	http://www.juniper.net/us/en/products-services/security/secure-analytics/
131	**Kratos - Ai Metrix, Inc.**	**NeuralStar**	NeuralStar is a two-tiered, centrally monitored, fully replicated enterprise IT management system that provides network continuity of operations out-of-the-box. • Delivers a global consolidated view of the entire network. • Provides visibility into remote deployments for a single view of geographically distributed networks. • Ensures automatic failover and redundancy for continuous operation. • Provides real-time intelligence by analyzing events in memory or in a database. • Monitors the health of the network by aggregating fault, availability and management data from multiple components. • Tracks application performance and availability across multiple installations in distributed environments. • Offers a more efficient and economical alternative to Manager of Managers (MOM) and Element Management Systems (EMS)	http://www.kratosnetworks.com/~/media/networks/pdf/neuralstar%20enterprise%20network%20manageme
132	**LogRhythm**	**LogRhythm SIEM**	LogRhythm SIEM is a solution that fully integrates Log Management and SIEM capabilities with deep Network and Endpoint Forensics capabilities. LogRhythm's next generation SIEM analyzes all available log and machine data and combines it with deep forensic data capture at both the server and network level for true enterprise visibility. This insight is leveraged by AI Engine, LogRhythm's patented Machine Analytics technology, to deliver automated, continuous analysis of all activity observed within the environment. The integrated architecture ensures that when threats and breaches are detected customers can quickly access a global view of activity enabling security intelligence and rapid response.	https://www.logrhythm.com/siem-2.0/logrhythm-security-intelligence/siem-with-logrhythm.aspx

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
133	**Lumeta Corporation**	**ESI**	Modern enterprise IT infrastructure is virtualized, leveraging private, public or hybrid "clouds" consisting of internal and external compute resources. And increasingly, enterprise network users are doing business on mobile platforms – smartphones, tablets and notebooks. Traditional security and vulnerability assessment (VA) products already miss at least 20% of what was physically hardwired to the network because they don't search for the unknown. Additionally, since VA scans stop, take too long to complete or consume too much network resource, they are often performed outside of normal business hours. This means IT security teams fail to gain cyber visibility into those mobile, virtual and cloud assets that simply aren't present at the time the VA scan is looking. Lumeta® Enterprise Situational Intelligence (ESI) offers real-time, context-driven security intelligence to address these problems. By enhancing Lumeta's Recursive Network Indexing techniques with the context of network state change via analysis of network control plane protocols (OSFP, BGP, ARP, DHCP, DNS, ICMPv6, and others), Lumeta ESI is able to provide authoritative network situational awareness, in real-time, as mobile, virtual, cloud assets and even the physical/software defined network itself changes.	http://www.lumeta.com/products/esi/
134	**Lumeta Corporation**	**Ipsonar**	Lumeta® IPsonar® leverages a suite of Recursive Network Indexing techniques to crawl the enterprise network and find the unknown and undocumented. This makes IPsonar the authoritative source for IP address space and network infrastructure visualization, routed and bridged topology, discovery of connected devices/profiles and cybersecurity anomalies that are really there, right now.	http://www.lumeta.com/products/ipsonar/
135	**McAfee**	**Advance Correlation Engine**	Sophisticated, dedicated threat detection based on risk and real-time data. Deploy McAfee Advanced Correlation Engine with McAfee Enterprise Security Manager to identify and score threat events in real time, using both rule- and risk-based logic.	http://www.mcafee.com/us/products/advanced-correlation-engine.aspx
136	**McAfee**	**Advanced Threat Defense**	McAfee Advanced Threat Defense detects targeted attacks and connects with existing defenses, converting threat intelligence into immediate action and protection. Unlike traditional sandboxes, it provides multiple analysis engines to broaden detection and expose evasive threats.	http://www.mcafee.com/us/products/advanced-threat-defense.aspx
137	**McAfee**	**Antivirus**	Shield your digital life and all your devices	https://www.mcafee.com/consumer/en-us/store/m0/catalog/mav_512/mcafee-antivirus-plus.html?pkgid=512
138	**McAfee**	**Application Control Product Family**	The McAfee Application Control blocks unauthorized executables on servers, corporate desktops, and fixed-function devices. Using a dynamic trust model and innovative security features, it thwarts advanced persistent threats—without requiring signature updates or labor-intensive list management.	http://www.mcafee.com/us/products/application-control.aspx
139	**McAfee**	**Application Data Monitoring**	McAfee Application Data Monitor detects fraud, data loss, and advanced threats by monitoring all the way to the application layer.	
140	**McAfee**	**Change Control Product Family**	The McAfee Change Control solution eliminates change activity in server environments that can lead to security breaches, data loss, and outages. McAfee Change Control makes it easy to meet regulatory compliance requirements. It allows for the protection of critical systems, configuration, and content files across distributed and remote locations by enabling instant change detection and providing sophisticated alerting mechanisms. It also prevents tampering with critical files and registry keys. It fulfills PCI DSS regulation requirements. It also prevents change-related outages and delays. It also eliminates manual and resource-intensive compliance policies.	http://www.mcafee.com/us/products/change-control.aspx
141	**McAfee**	**Content Security (Email and Web Protection)**	McAfee Content Security Suite. Comprehensive email, web, and data security	http://www.mcafee.com/us/products/web-security/index.aspx
142	**McAfee**	**Data Loss Prevention**	McAfee Complete Data Protection Suites and McAfee Data Loss Prevention (DLP) solutions provide multilayered protection for data regardless of where it resides—on the network, in the cloud, or at the endpoint.	http://www.mcafee.com/us/products/data-protection/index.aspx
143	**McAfee**	**DB Event Monitor**	McAfee Database Event Monitor for SIEM provides a complete audit trail of all database activities, including queries, results, authentication activity, and privilege escalations.	http://www.mcafee.com/us/products/database-event-monitor-for-siem.aspx
144	**McAfee**	**Enterprise Log Manager**	McAfee Enterprise Log Manager collects, compresses, signs, and stores all original events with a clear audit trail of activity that can't be repudiated.	http://www.mcafee.com/us/products/enterprise-log-manager.aspx
145	**McAfee**	**Enterprise Security Manager**	McAfee Enterprise Security Manager delivers a real-time understanding of the world outside—threat data, reputation feeds, and vulnerability status—as well as a view of the systems, data, risks, and activities inside your enterprise.	http://www.mcafee.com/us/products/enterprise-security-manager.aspx
146	**McAfee**	**ePO Product Family**	McAfee ePolicy Orchestrator (McAfee ePO) is an advanced, extensible, and scalable centralized security management software that allows for: a unified view of your security posture with drag-and-drop dashboards that provide security intelligence across endpoints, data, mobile and networks; simplified security operations with streamlined workflows for proven efficiencies; flexible security management options that allow you to select either a traditional premises-based or a cloud-based management version of McAfee ePO; and leverage of existing third-party IT infrastructure from a single security management console with our extensible architecture.	http://www.mcafee.com/us/products/epolicy-orchestrator.aspx
147	**McAfee**	**ePolicy Orchestrator**	A single console for all your security management. McAfee ePolicy Orchestrator (McAfee ePO) is the most advanced, extensible, and scalable centralized security management software in the industry. Get a unified view of your security posture with drag-and-drop dashboards that provide security	http://www.mcafee.com/us/products/epolicy-orchestrator.aspx
148	**McAfee**	**Event Receiver**	Collect up to tens of thousands of events per second. McAfee Event Receiver collects and retains large amounts of security data, and gives you immediate access to that data.	http://www.mcafee.com/us/products/event-receiver.aspx
149	**McAfee**	**Global Threat Intelligence**	Based on activity from millions of sensors world-wide and an extensive research team, McAfee Labs publishes timely, relevant threat activity via McAfee Global Threat Intelligence (GTI). This always-on, cloud-based threat intelligence service enables accurate protection against known and fast-emerging threats by providing threat determination and contextual reputation metrics.	http://www.mcafee.com/us/threat-center/technology/global-threat-intelligence-technology.aspx
150	**McAfee**	**HIPS Product Family**	The McAfee Host Intrusion Prevention for Server is a solution that boosts server security and lowers costs by reducing the frequency and urgency of patching. It leverages powerful behavioral and signature analysis, plus a dynamic stateful firewall supported by cloud-based McAfee Global Threat Intelligence, to block emerging attacks in real time. It protects against exploits that target new vulnerabilities, so IT staff has more time for planning, testing, and deploying patches. It also maintains server uptime with specialized protection for web and database servers.	http://www.mcafee.com/us/products/host-ips-for-server.aspx

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
151	**McAfee**	**Management for Optimized Virtual Environments (MOVE) AntiVirus**	McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus brings advanced virus protection to virtualized desktops and servers, both on premises and in the cloud. Choose one efficient solution for virtual server and desktop security that works across multiple vendor platforms, or an agentless, tuned option for VMware NSX and VMware vShield.	http://www.mcafee.com/us/products/move-anti-virus.aspx
152	**McAfee**	**Policy Auditor Product Family**	The McAfee Policy Auditor is a software solution that automates security audit processes and helps report consistently and accurately against internal and external policies. It runs consolidated audits across both managed (agent-based) and unmanaged (agentless) systems, unifies the management of policy audits and endpoint security, gives up-to-date data through dashboards and reports, as well as built-in waiver management to simplify every step, and leverages predefined templates and controls to ease deployment and management.	http://www.mcafee.com/us/products/policy-auditor.aspx
153	**McAfee**	**Real Time Command**	McAfee Real Time Command revolutionizes security and systems management with immediate visibility into data and instant interventions. This powerful solution lets customers use plain English to find facts quickly and exert control over their IT environment with confidence. From stalking targeted malware and forbidden applications to large-scale remediation of noncompliance, McAfee Real Time Command empowers administrators to manage incident response, outbreaks, patching issues, security policies, and software compliance proactively.	http://www.sans.org/reading-room/whitepapers/analyst/improving-security-management-real-time-queries-34
154	**McAfee**	**Risk Advisor**	Complete visibility into your risk posture	http://www.mcafee.com/us/solutions/risk-management/index.aspx
155	**McAfee**	**SaaS Web & Email Protection**	Web protection solutions from Intel Security simplify and secure access to cloud applications while protecting organizations against advanced malware and other hidden threats. From granular application control to web filtering, deep content inspection, and advanced malware protection, Intel Security provides the industry's most comprehensive web security solution.Products include: McAfee Web Protection, McAfee Web Gateway, McAfee SaaS Web Protection	http://www.mcafee.com/us/products/web-security/index.aspx
156	**McAfee**	**SIEM Product Family**	The McAfee security information and event management (SIEM) solution brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and extensible compliance reporting. At the core of the SIEM offering, Enterprise Security Manager consolidates, correlates, assesses, and prioritizes security events for both third-party and McAfee solutions. As part of the Security Connected framework, McAfee Enterprise Security Manager tightly integrates with McAfee ePolicy Orchestrator (McAfee ePO) software, McAfee Risk Advisor, and Global Threat Intelligence — delivering the context required for autonomous and adaptive security risk management.	http://www.mcafee.com/us/products/siem/index.aspx
157	**McAfee**	**Threat Intel Exchange**	Leveraging the McAfee Data Exchange Layer (DXL), McAfee Threat Intelligence Exchange combines multiple threat information sources, and instantly shares this data out to all your connected security solutions, including third-party solutions. It provides adaptive threat detection on unknown files, resulting in faster time to protection and lower costs.	http://www.mcafee.com/us/products/threat-intelligence-exchange.aspx
158	**McAfee**	**Vulnerability Manager**	In October 2015, Intel Security announced the end of life (EOL) for McAfee Vulnerability Manager, a web application scanner, with the end-of-sale date in January 2016. This EOL process helps ensure we are investing in the right areas to continually innovate and lead the market with the best solutions that address our customers' security needs. Instead of directly participating in the vulnerability management segment, Intel Security has partnered with Rapid7 to transition our customers over to its market-leading Nexpose solution.	http://www.mcafee.com/us/products/vulnerability-manager-end-of-life.aspx
159	**Microsoft**	**System Center**	Microsoft System Center 2012 R2 helps you realize the benefits of the Microsoft Cloud OS by delivering unified management across your datacenters, service provider datacenters, and Windows Azure. With System Center 2012 R2 you can: * utilize enterprise-grade management capabilities with best-in-class performance for your Windows Server environments and first-party Microsoft workloads (SQL, Exchange, and SharePoint). * reduce datacenter complexity by simplifying how you provision, manage, and operate your infrastructure. * enable delivery of predictable application SLAs through a relentless focus on optimizing your applications and workloads.	http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/
160	**Novell**	**NetIQ Access Manager**	As demands for secure web access expand and delivery becomes increasingly complex, organizations face some formidable challenges. Access Manager™ provides a simple yet secure and scalable solution that can handle all your web access needs—both internal as well as in the cloud.	https://www.netiq.com/products/access-manager/
161	**Novell**	**NetIQ Advanced Authentication for SecureLogin**	Often, when an organization commits and invests their time and resources in a two factor authentication solution, they do so to meet their needs at the time. Too often, that same organization finds themselves implementing yet another solution to meet new needs. All too often it happens yet again, but rest assured, there is a better way	https://www.netiq.com/products/advanced-authentication-framework/
162	**Novell**	**NetIQ Identity Manager Integration Module**	Identity Manager delivers a complete, yet affordable solution to control who has access to what across your enterprise—both inside the firewall and into the cloud. It enables you to provide secure and convenient access to critical information for business users, while meeting compliance demands.	https://www.netiq.com/products/identity-manager/advanced/
163	**Novell**	**Secure Login**	SecureLogin streamlines user authentication for enterprise applications by providing a single login experience to the users. It eliminates password reset calls, protects against unauthorized access to business applications, and integrates with almost any authentication device.	https://www.netiq.com/products/securelogin/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
164	**Oracle**	**Access Manager**	Oracle Access Management provides innovative new services that complement traditional access management capabilities. For example, adaptive authentication, federated single-sign on (SSO), risk analysis, and fine-grained authorization are extended to mobile clients and mobile applications, and Access Portal allows customers to build their own private cloud SSO services. Services can be licensed and enabled as required to meet the specific needs of your organization. * Access Management's server-side services hosted in Oracle WebLogic Server. * Access Management's first-line-of-defense interceptors and filters (Access Management WebGates, and Web Services and API Gateway) * Mobile and Social service client SDK, installed on mobile devices. * Enterprise SSO Suite installed on PCs (desktops and laptops). * Web Services Manager's client agents embedded in web services or applications sending requests to web services providers in the Application Tier. * Directory services may alternatively be deployed in the Data Tier (Note: Oracle Directory Services are not part of the Oracle Access Management Suite, they're sold separately).	http://www.oracle.com/us/products/middleware/identity-management/access-management/overview/index.
165	**Oracle**	**Advanced Security**	Comply with privacy and regulatory mandates that require encrypting and redacting (display masking) application data, such as credit cards, social security numbers, or personally identifiable information (PII). By encrypting data at rest and masking data whenever it leaves the database, Oracle Advanced Security provides the most cost-effective solution for comprehensive data protection	http://www.oracle.com/us/products/database/options/advanced-security/overview/index.html
166	**Oracle**	**API Gateway**	Oracle API Gateway is a standards-based, policy-driven, standalone software security solution that provides first line of defense in Service-Oriented Architecture (SOA) environments. It enables organizations to securely and rapidly adopt Cloud, Mobile, and SOA Services by bridging the gaps and managing the interactions between all relevant systems.	http://www.oracle.com/us/products/middleware/identity-management/api-gateway/overview/index.html
167	**Oracle**	**Business Intelligence Server**	Oracle Business Intelligence Enterprise Edition (OBIEE) is a comprehensive business intelligence platform that delivers a full range of capabilities - including interactive dashboards, ad hoc queries, notifications and alerts, enterprise and financial reporting, scorecard and strategy management, business process invocation, search and collaboration, mobile, integrated systems management and more. OBIEE is based on a web service-oriented unified architecture that integrates with an organization's existing information technology (IT) infrastructure for the lowest total cost of ownership (TCO) and highest return on investment (ROI).	http://www.oracle.com/technetwork/middleware/bi-enterprise-edition/overview/index.html
168	**Oracle**	**Data Integrator Enterprise Edition**	Oracle Data Integrator Enterprise Edition delivers high-performance data movement and transformation among enterprise platforms with its open and integrated E-LT architecture and extended support for Big Data. Oracle Data Integrator Enterprise Edition is critical to leveraging data management initiatives on-premise or in the cloud, such as big data management, Service Oriented Architecture and Business Intelligence. Oracle Data Integrator Enterprise Edition is fully integrated with Oracle Fusion Middleware, Oracle GoldenGate, Oracle Database, and Exadata to put data at the center of your enterprise. Oracle Data Integrator Enterprise is open and standards-based to work with 3rd Party applications as well as Oracle's applications.	http://www.oracle.com/us/products/middleware/data-integration/enterprise-edition/overview/index.html
169	**Oracle**	**Directory Services Plus**	Oracle Unified Directory is an all-in-one Java-based directory solution with storage, proxy, synchronization and virtualization capabilities. While unifying the approach, it provides all the services required for high-performance Enterprise and carrier-grade environments. Oracle Unified Directory is part of Oracle Directory Services Plus. It ensures scalability to billions of entries, ease of installation, elastic deployments, enterprise manageability and effective monitoring.	http://www.oracle.com/us/products/middleware/identity-management/directory-services/overview/index.htm
170	**Oracle**	**Enterprise Identity Services Suite**	Oracle's award-winning identity management offerings are available as a comprehensive identity management suite. With cost-effective, per-user pricing, this suite provides flexibility for the future.	http://www.oracle.com/us/products/middleware/identity-management/oiam/overview/index.html
171	**Oracle**	**Enterprise Single Sign-On Suite**	Single Sign-On from Desktop to Cloud. A suite of best-in-class products that simplifies enterprise single sign-on deployments for system administrators and extends the benefits of ESSO to remote and mobile users.	http://www.oracle.com/us/products/middleware/identity-management/oracle-enterprise-sso/overview/index
172	**Oracle**	**Entitlements Server**	Oracle Entitlements Server is an entitlements system that supports the centralized definition of complex application entitlements and the distributed runtime enforcement of those entitlements. It allows you to externalize entitlements – remove security decisions from the application. It provides the means to define application resources and application businesses objects, represent those objects in hierarchical relationships, and write policies that describes which users, groups and roles can access those objects. You can write policies that control access to both application software components as well as arbitrary business objects in the application. Oracle Entitlements Server also includes a security integration framework that provides an easy way to integrate with existing authentication, Web SSO, identity management, and user provisioning systems.	http://docs.oracle.com/cd/E12890_01/ales/docs32/secintro/oes.html
173	**Oracle**	**Identity and Access Management Suite**	Oracle's award-winning identity management offerings are available as a comprehensive identity management suite. With cost-effective, per-user pricing, this suite provides flexibility for the future. * An integrated suite that enables faster deployments and streamlined day-to-day operations * Proven, best-in-class solutions abstract and centralize security for applications and Web services * A single solution that cuts TCO * Enables organizations to expand identity management projects beyond their initial scope * Cuts the time spent integrating disparate components * Provides a single point of contact for support, a single license contract, and the backing of the world's largest enterprise software company	http://www.oracle.com/us/products/middleware/identity-management/oiam/overview/index.html

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
174	**Oracle**	**Identity Federation**	Oracle Identity Federation (OIF) is a complete, enterprise-level solution for secure identity information exchange between partners. OIF reduces account management for partner identities and lowers the cost of integrations through support of industry federation standards. Oracle Identity Federation protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications. Oracle Identity Federation 11g R2 is now a shared service of the Oracle Access Management platform, enabling seamless integration of SAML attributes and Oracle Access Manager policies. Oracle Identity Federation 11g R2 enables enterprises to quickly implement cross-domain SSO by providing an end-to-end federation solution, including Oracle OpenSSO Fedlet, a simple and lightweight deployment option for onboarding service providers.	http://www.oracle.com/technetwork/middleware/id-mgmt/index-084079.html
175	**Oracle**	**Identity Governance Suite**	The industry's most comprehensive identity governance solution delivers user administration, privileged account management, and identity intelligence, powered by rich analytics and actionable insight. * Actionable identity intelligence through automated controls, rich dashboards, and risk-based analytics that controls enterprise risk and enables rapid compliance * Business-friendly, role-based identity administration automates user provisioning for both on-premise and cloud applications * Privileged account management controls access from shared accounts and delivers a rich audit trail, ensuring enhanced security and compliance for sensitive systems	http://www.oracle.com/us/products/middleware/identity-management/governance/overview/index.html
176	**Oracle**	**Identity Manager**	Oracle Identity Manager is a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise IT resources. Its flexible architecture easily handles the most uncompromising and rigorous IT and business requirements -- without requiring changes to existing infrastructure, policies or procedures. Oracle Identity Manager is designed to manage user access privileges across all of a firm's resources, throughout the entire identity management lifecycle -- from initial creation of access privileges to dynamically adapting to changes in business requirements. Because of Identity Manager's innovative design, enterprises can elegantly incorporate necessary business changes at minimal cost, while avoiding enforced customization that might be necessary with other provisioning systems.	http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-098451.html
177	**Oracle**	**Mobile Security Suite**	Oracle Mobile Security Suite provides a comprehensive Enterprise Mobility Management (EMM) solution (Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM), and Mobile Identity) that can address a mix of both Bring Your Own Device (BYOD) and corporate owned models without compromising security, user experience or privacy. This EMM solution enables organizations to move to a "Mobile First" strategy as part of the complete Oracle Mobile Platform, to build feature rich, cross platform, integrated apps and leverage an advanced and industry leading Oracle Identity and Access Management solution for securing corporate access.	http://www.oracle.com/us/products/middleware/identity-management/mobile-security/overview/index.html
178	**Oracle**	**SOA Suite**	Ocracle SOA Suite is a comprehensive, standards-based software suit to build, deploy and manage integration following the concepts of service-oriented architecture (SOA). The components of the suite benefit from consistent tooling, a single deployment and management model, end-to-end security and unified metadata management. The functional components of Oracle SOA Suite are grouped in four broad categories: connectivity, service virtualization, orchestration, and analytics.	http://www.oracle.com/us/products/middleware/soa/suite/overview/index.html
179	**Oracle**	**WebLogic Server Management Pack Enterprise**	The WebLogic Server Management Pack Enterprise Edition greatly improves server as well as application performance by providing unique functionality to automatically detect performance bottlenecks; quickly diagnose these performance problems, and identify their root cause.	http://www.oracle.com/technetwork/oem/soa-mgmt/index.html
180	**Palo Alto Networks**	**Global Protect subscription**	Safely enable the mobile workforce by using GlobalProtect to deliver the protection of the our next-generation security platform to laptops, smartphones and tablets.	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions
181	**Palo Alto Networks**	**Next Generation Firewalls**	Our next-generation firewall is the only one that attempts to fully classify traffic (including user association), and then make all of that classification knowledge available to all control and enforcement options. It's an approach that allows for precise, flexible control of traffic based on: applications, users, and the information content of the traffic. In addition to control and security capability, our next-generation firewalls are designed for operations. Our simple, straightforward user interface complements the straightforward architecture. Automation and integration into larger systems (e.g., automated provisioning, SDN) is supported by our XML API.	https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall
182	**Palo Alto Networks**	**PANDB URL filtering site license subscription**	The perfect complement to the policy-based application control provided by App-ID™ is our on-box URL filtering database, which gives you total control over Web-related activity, including the ability to prevent users from visiting malicious websites.	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions
183	**Palo Alto Networks**	**Panorama Network Security management**	Network security management empowers you with easy-to-implement, consolidated policy creation and management. Set up and control firewalls centrally with industry-leading functionality and an efficient rule base, and gain insight into network-wide threats while correlating information across your entire network.	https://www.paloaltonetworks.com/products/secure-the-network/management
184	**Palo Alto Networks**	**Threat prevention subscription**	Because application context and SSL decryption are basic features of our firewalls, you're able to inspect and stop threats "hiding" within them. You're also able to view threat logs within the context of applications, so you can fully understand the risk posed by specific applications.	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
185	**Palo Alto Networks**	**Traps Advanced Endpoint Protection (Secure the Endpoint)**	This new approach needs to prevent advanced attacks originating from executables, data files or network-based exploits – known and unknown – before any malicious activity could successfully run. We call this "advanced endpoint protection." By focusing our solution on the attacker's core techniques and putting up barriers to mitigate them, the attacker's path for exploitation becomes known, even when the attack isn't.	https://www.paloaltonetworks.com/products/secure-the-endpoint/traps
186	**Palo Alto Networks**	**Virtual Next Generation Firewalls**	Just as an attack or compromise within your physical data center is a significant incident, the impact of a compromise in your virtualized environment is amplified because your workloads, some of which use varied trust levels, and the associated data are centralized, without any security barriers in between to keep them segmented. If your virtual environment is compromised, the attacker has access to your entire virtualized environment. VM-Series includes: VM-Series for AWS ; VM-Series for Citrix ; VM-Series for KVM & OpenStack ; VM-Series for VMware NSX ; VM-Series for VMware ESXi/vCloud Air	https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall
187	**Palo Alto Networks**	**WildFire subscription**	WildFire™ cloud-based malware analysis environment offers advanced protection from unknown threats. Through native integration with our next-generation security platform, the service brings advanced threat detection and prevention to every security appliance deployed throughout the network, automatically sharing protections with all subscribers globally in about 15 minutes.	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions
188	**Pentaho**	**Adaptive Big Data**	Within a single platform, our solution provides big data tools to extract, prepare and blend your data, plus the visualizations and analytics that will change the way you run your business. From Hadoop and NoSQL to analytic databases, Pentaho allows you to turn big data into big insights.	http://www.pentaho.com/product/big-data-analytics
189	**Pentaho**	**Data Integration**	Pentaho data integration prepares and blends data to create a complete picture of your business that drives actionable insights. The platform delivers accurate, "analytics ready" data to end users from any source. With visual tools to eliminate coding and complexity, Pentaho puts big data and all data sources at the fingertips of business and IT users.	http://www.pentaho.com/product/data-integration
190	**Qualys**	**QualysGuard**	The Qualys Cloud Platform, also known as QualysGuard, consists of an integrated suite of solutions to help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Delivered via a multi-tenant shared cloud service or a private cloud, the Qualys Cloud Platform or QualysGuard is the first security platform that provides you with continuous security and allows you to monitor, detect and protect your global network – from the perimeter to the core.	https://www.qualys.com/qualysguard/
191	**Radiant Logic**	**Cloud Federation Service (CFS)**	RadiantOne Cloud Federation Service is a soltuion that delegates the task of authenticating an organizations identity stores to one common virtual layer and shields external and cloud applications from the complexity of identity systems.	http://www.radiantlogic.com/products/radiantone-cfs/
192	**Radiant Logic**	**Identity Correlation & Synchronization Server (ICS)**	RadiantOne correlates and disambiguates same-users across these data silos, creating a union set of identities where duplicate user accounts are joined to create a global profile. The global profile provides a single representation for all users across multiple systems, linked to each of the underlying profiles. With our powerful correlation technology, it's easy to: * Handle overlapping attributes: When dealing with a heterogeneous environment, identity information is often duplicated in multiple repositories. Same-user profiles may also contain contradictory attribute names and values, or may be in different formats. It is essential that consuming applications be given the correct information, in the expected format. * Disambiguate attributes and map to unique names: Often, same-named attributes need to be defined differently—or re-named—depending on the correct context. They are not interchangeable and must be disambiguated within the system. * Return multi-valued attributes: If multiple values for an attribute exist in different systems, VDS can return a multi-valued attribute. * Return attributes based on authoritative source: RadiantOne can also return attributes based on priority. This enables administrators to set precedence for attribute value sources, ensuring only most authoritative data available is presented.	http://www.radiantlogic.com/solutions/portal-security-solutions/unify-identity-representation/correlate-ident
193	**Radiant Logic**	**Virtual Directory Server (VDS)**	RadiantOne VDS is a sophisticated virtualization platform designed to address the complexity of today's identity environments. It comes with two licensing options, both of which share many of the advanced capabilities from proxy-driven routing and remapping engine to a model-driven virtualization solution as well as SQL access, contextual views for complex attribute-driven authorization and personalization, and real-time cache refresh.	http://www.radiantlogic.com/products/radiantone-vds/
194	**Rapid 7**	**METASPLOIT**	Metasploit, backed by a community of 200,000 users and contributors, gives you that insight. It's the most impactful penetration testing solution on the planet. With it, uncover weaknesses in your defenses, focus on the highest risks, and improve your security outcomes. Simulate real-world attacks to find your weak points before a malicious attacker does. Metasploit Pro seamlessly enables you to leverage the Metasploit® open–sourced frame for reconnaissance and exploitation modules speeding up your penetration test. Use attacker techniques to evade anti-virus, find weak credentials, and pivot throughout the network.	http://www.rapid7.com/products/metasploit/
195	**Rapid 7**	**NEXPOSE**	Rapid7's vulnerability management solution, Nexpose, helps you reduce your threat exposure by prioritizing risk across vulnerabilities, configurations, and controls with awareness of the threat landscape across the modern network. Data breaches are growing at an alarming rate. Your attack surface is constantly changing, the adversary is becoming more nimble than your security teams, and your board wants to know what you are doing about it. Nexpose gives you the confidence you need to understand your attack surface, focus on what matters, and create better security outcomes.	http://www.rapid7.com/products/nexpose/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
196	**Red Hat**	**Certificate System**	A scalable, secure platform for public key infrastructure. Red Hat® Certificate System is an enterprise software system that gives you a scalable, secure framework to establish and maintain trusted identities and keep communications private. Red Hat Certificate System provides certificate life-cycle management—issue, renew, suspend, revoke, archive and recover, and manage single and dual-key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications.	https://www.redhat.com/en/technologies/cloud-computing/certificate-system
197	**Red Hat**	**Directory Server**	Red Hat Directory Server is an LDAP-compliant server that centralizes application settings, user profiles, group data, policies, and access control information into a network-based registry	https://www.redhat.com/f/pdf/rhas/DirSecProductSheetDirectoryServer.pdf
198	**Red Hat**	**jBoss Business Rules Management System (BRMS)**	JBoss BRMS enables your organization to: Deploy decision services across physical, virtual, and cloud environments. Improve business agility. Make consistent and efficient decisions. Quickly build resource optimization solutions. Shorten development cycles for faster time to market.	https://www.redhat.com/en/technologies/jboss-middleware/business-rules
199	**RedSeal, Inc.**	**RedSeal 4205 Appliance**	The RedSeal 4205 appliance provides a secure, easy to deploy means of implementing RedSeal software. While other products can give you a snapshot of your network, only RedSeal lets you see your “as built” network and determines your security priorities. RedSeal’s advanced analytics engine creates an accurate model of your network by examining device configurations, scanner data, vulnerability databases, and host information. It includes the virtual (Cloud-based, SDN) parts of your network as well as the physical. RedSeal then centralizes and integrates this information, first verifying that your network complies with industry best practices, then testing it to identify security risks. Most importantly, RedSeal prioritizes needed security actions—in the context of your network -- and gives you the critical information you need to quickly remediate issues. And it does this automatically and continuously. As a result, you are able to use your scarce resources to address your most critical security issues first and continuously monitor your network.	https://redseal.co/content/product
200	**RedSeal, Inc.**	**RedSeal STIG Checks**	Department of Defense. Increase network resilience with RedSeal across the DoD by enabling proactive defense and predictive analysis.	https://redseal.co/government/
201	**RES**	**IT Store**	Organizations can improve operational efficiency by automating business processes and IT service delivery. The RES ONE Service Store is lightweight and easily integrates with an organization’s existing technology, maximizing earlier investments without requiring expensive "rip and replace" projects. RES can serve as a central identity warehouse, allowing IT teams to manage access by aggregating information from a variety of sources. RES ONE Service Store lays the foundation for IT to speak with the business on the right terms – as a strategic service provider.	http://www.ressoftware.com/product/res-one-service-store
202	**RES**	**ONE Workspace**	RES ONE Workspace offers today’s digital workforce a better, more personalized technology experience, while giving IT the control to increase security and reduce costs. In today’s complex IT environments, traditional tools often falls short in providing a smooth and seamless experience. The result is often unhappy employees and your IT staff overrun with service desk tickets. Workspace management goes beyond profile management to deliver a consistent experience across desktop delivery platforms and a dynamic workspace with the right mix of apps and services to maximize the productivity of your workforce.With RES ONE Workspace, each workspace becomes personalized and context aware, optimized based on time, location, device and more, so mobile workers are equally enabled and secure.	http://www.ressoftware.com/product/res-one-workspace
203	**RES**	**Suite 2014**	RES ONE Suite takes a people-centric approach to business technology, empowering the workforce through self-service and automated delivery and return of the right apps and services to each person’s secure digital workspace. With RES Suite, technology is delivered to employees proactively and securely, building a foundation for IT as a Service (ITaaS) to support today’s agile workplace. RES ONE offers: •Automatic delivery and return of services based on each user’s real-time working context •The ability to predict (and deliver) what services a user will likely need at a given time and place •A consumer-like self-service experience for all other requests that aren’t predicted	http://www.ressoftware.com/product/res-one-suite-2015
204	**RSA**	**Access Fulfilllment Express**	Rapidly and reliably execute user access changes, without manual effort.lose the “provisioning gap” by fulfilling changes across all key applications and data sources. Utilize pre-built adapters for rapid on-boarding of applications and data sources. Easily connect to custom applications via configuration-based adapters, avoiding long and expensive adapter development projects. Leverage existing provisioning systems without the need to rip and replace such investments. Achieve fast time-to-value through rapid project deployments. Provision access to both SaaS and on-premise applications from the cloud.	https://www.emc.com/collateral/data-sheet/h12510-ds-rsa-access-fulfillment-express.pdf

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
205	**RSA**	**Archer Assessment and Authorization**	The RSA Archer Assessment & Authorization (A&A) solution is an ideal foundation for a comprehensive RSA Archer-based IA Management suite. It serves as the system of record for every person, location, component, and tier in an organization, as well as every piece of hardware and software and every information asset. The A&A solution manages the full cycle of NIST RMF (800-37) activities.	http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-assessment-authorization-fe
206	**RSA**	**Archer Federal Continuous Monitoring**	The RSA Archer Continuous Monitoring (CM) solution provides several capabilities including near-real-time insight into the security posture of every device in the enterprise. As well as capabilities that allow an agency/department to determine if controls are implemented and operating as targeting individual high-risk devices, the RSA Archer CM solution can inform the Authorizing Official (AO) on a wide range of risk decisions for Assessment & Authorization (A&) and FISMA compliance activities.	http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-continuous-monitoring-fede
207	**RSA**	**Archer GRC Suite**	The RSA Archer GRC Platform supports business-level management of enterprise governance, risk management, and compliance (GRC). As the foundation for all RSA Archer offerings, our Platform allows you to adapt each product to your requirements, build your own applications, and integrate with other systems without touching code. Archer GRC Products including: Compliance User;Enterprise User;Fed Enterprise; Incident User; Policy User; Risk User; Threat User	http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-platform.htm - !details
208	**RSA**	**Business Role Manager**	RSA® Business Role Manager helps organizations deploy effective role-based access control, which streamlines access delivery and simplifies access compliance.	https://www.rsa.com/en-us/perspectives/resources/business-role-manager-ds
209	**RSA**	**Data Access Governance (DAG)**	It is critical to extend access governance to unstructured data as well as structured data in order to reduce access-related risk and enhance compliance efforts. RSA Data Access Governance (DAG) provides ubiquitous access governance support across all major file systems and Microsoft® SharePoint®, giving you one place to centrally manage and govern access.	https://www.rsa.com/en-us/search?q=Data%20Access%20Governance&pageNumber=1
210	**RSA**	**Identity Management and Governance (IMG)**	The RSA IMG platform helps organizations efficiently meet their security, regulatory, and business access needs, through a collaborative set of business processes. By automating manual tasks, providing evidence of compliance, reducing access-related business risk, and efficiently delivering business access, enterprises can confidently manage, control, and enforce access to applications and data, across the enterprise and the cloud.	http://www.emc.com/collateral/data-sheet/h12512-ds-rsa-iam-platform.pdf
211	**RSA**	**NetWitness Series 4**	Through the unique combination of network, log, identity and endpoint data, detect, investigate, and rapidly respond to advanced threats before they damage the business.	https://www.rsa.com/en-us/products-services/security-operations
212	**RSA**	**SecurID On-Demand Authenticaton**	RSA SecurID provides world-leading two-factor authentication, protecting 25,000 organizations and 55 million users. RSA SecurID extends security to bring your own device (BYOD), cloud, and mobile as well as traditional virtual private network (VPN) and web portals. RSA SecurID solutions comprise three primary components: authenticator, platform, and agents.	https://www.rsa.com/en-us/products-services/identity-access-management/securid
213	**RSA**	**Security Analytics**	To detect advanced attacks, logs need to be combined with other data types such as network packet, endpoint, and cloud data. RSA Security Analytics discovers attacks missed by log-centric SIEM and signature-based tools with the only solution that can correlate network packets with other security data.	https://www.rsa.com/en-us/products-services/security-operations/security-analytics
214	**RSA**	**Security Operations Management**	RSA Acrcher Security Operations Management is a software solution that enables enterprises to orchestrate people, process, and technology to effectively respond to security incidents and prepare for a data breach. It leverages industry best practices that allows the Security Operations Management to provide a framework for customers building a security operations center (SOC).	http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-security-operations-manage
215	**RSA**	**Software as a service (SaaS) Single Sign On (SSO)**	RSA Via Access applies single sign-on across external SaaS, internal Web, or custom applications, and Security Assertion Markup Language (SAML)-enabled native mobile applications for a truly unified user experience.	https://www.emc.com/security/rsa-via-access.htm#!
216	**RSA**	**Vulnerability Risk Management**	RSA Archer Vulnerability Risk Management takes a big data approach to helping security teams identify and prioritize high-risk threats. Built on the RSA Archer platform, Vulnerability Risk Management helps organizations proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results, and comprehensive workflows. The Vulnerability Analytics investigative interface allows IT security analysts to get alerts, explore results, and analyze issues as they arise. A powerful and flexible rules engine highlights new threats, overdue issues, and changing business needs. For business and IT managers, Vulnerability Risk Management's management module integrates Vulnerability Risk Management analytics with reporting, workflows, and a risk-management framework to enable data-driven security decisions.	http://www.emc.com/security/rsa-archer-governance-risk-compliance/rsa-archer-vulnerability-risk-manageme

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
217	**SailPont Technologies**	**SailPoint IdentityIQ**	IdentityIQ is SailPoint's governance-based Identity and Access Management (IAM) software solution that delivers a unified approach to compliance, password management and provisioning activities for applications running on-premises or from the cloud. IdentityIQ meets the needs of large organizations with complex IAM processes who prefer to tailor their solution to align with unique business needs. * Access Certification for IdentityIQ: Automates access certifications to improve audit performance and reduce the cost and burden of compliance. * Self-Service Access Request for IdentityIQ: Empowers users to request and manage access on their own, with automatic policy enforcement. * Password Management for IdentityIQ: Enables users to reset and change passwords without having to call the help desk, while enforcing strong password policy. * Automated Provisioning for IdentityIQ: Fully automates user provisioning to streamline access changes based on user requests or detected user lifecycle events. * Governance Platform for IdentityIQ: Centralizes identity data and leverages one model for policy, risk, and roles across all IAM processes. * Identity Intelligence for IdentityIQ: Highlights business-relevant information in easy-to-understand dashboards, reports, and advanced analytics. * Enterprise Integration for IdentityIQ: Provides flexible connectivity and integration to third party solutions that enhances IT security and operations.	https://www.sailpoint.com/products/identityiq
218	**ServiceNow**	**CreateNow Development Suite**	ServiceNow CreateNow Development Suite provides a consolidated and comprehensive set of browser-based tools to manage the entire lifecycle of an application from creation to deployment. And the completed application can easily be deployed to a single department or your entire enterprise with the click of a button.	http://www.servicenow.com/products/service-automation-platform/createnow-development-suite.html
219	**ServiceNow**	**Discovery Application**	ServiceNow Discovery identifies IP-enabled configuration items (CIs), maps their interdependencies, and populates and maintains them in the ServiceNow Configuration Management Database (CMDB) – a critical step to automating service management. Discovery is scheduled on a regular basis to help ensure the accuracy of the CI data underpinning all ServiceNow IT service automation applications across the enterprise.	http://www.servicenow.com/products/discovery.html
220	**ServiceNow**	**Implementation Services**	ServiceNow provides customers with a portfolio of services – a powerful combination of ITSM best practices and a proven implementation methodology – that covers all aspects of a customer's ServiceNow lifecycle. Customers can either tailor their implementation with a customized deployment plan based on their processes or select from application-specific packages called QuickStarts, which focus on specific processes and applications, and take an iterative, modular approach to driving IT transformation across the business.	http://www.servicenow.com/services/implementation-services.html
221	**ServiceNow**	**IT Service Automation Suite**	ServiceNow Service Automation Platform is a highly configurable, extensible, and easy-to-use cloud application platform built on an enterprise-grade cloud infrastructure. All ServiceNow applications, as well as new applications created by ServiceNow customers and partners, are developed on this common, underlying platform. All of these applications leverage one user interface, one code base and one data model to create a single system of record.	http://www.servicenow.com/products/service-automation-platform.html
222	**ServiceNow**	**Orchestration Cloud Provisioning**	ServiceNow Cloud Provisioning enables IT to automate the entire cloud management lifecycle. From self-service cloud selection to automated, standardized cloud creation and resource optimization, cloud provisioning speeds the deployment of Amazon EC2 and VMware vSphere cloud environments from weeks or months to just minutes. Without special training or manual intervention, cloud administration is transformed from day-to-day IT management overhead to an automated business self-service – all within parameters determined by IT.	http://www.servicenow.com/products/orchestration/cloud-provisioning.html
223	**ServiceNow**	**Orchestration Core**	ServiceNow Orchestration automates the processes that involve systems and applications outside of the ServiceNow environment which can include can be simple or complex tasks across remote applications, services, and infrastructure for IT operations management, process automation, and business automation scenarios.	http://www.servicenow.com/products/orchestration.html
224	**ServiceNow**	**Performance Analytics Application**	ServiceNow Performance Analytics application is a solution that allows visualization of KPIs and metrics related to any service management process. It automates recurring metric reporting needs and gives actionable performance scorecards to drill down and evaluate metrics.	http://www.servicenow.com/products/performance-analytics.html
225	**ServiceNow**	**Service Automation Platform**	Applications built on ServiceNow's application-platform-as-a-service (aPaaS) can be used to automate more processes and replace software deployments with service delivery in the cloud.	http://www.servicenow.com/products/servicenow-platform.html
226	**ServiceNow**	**ServiceWatch**	ServiceNow ServiceWatch has an innovative, "top-down" approach to discovering and mapping the relationships between IT components that comprise specific business services, even in dynamic, virtualized environments. Dashboards provide insights into the health of business services in real time, correlate service issues with infrastructure events, and contain metrics that alert based on business impact. ServiceWatch uses component-specific monitoring data from third-party systems to correlate incidents to impacted business services.	http://www.servicenow.com/products/servicewatch.html
227	**Sightline Holdings Corp.**	**ACE: Security & Compliance Module**	ACE: Security & Compliance Module. Sightline ACE is a complete, single-pane monitoring solution that gives users real-time insight into data center and cloud resources. Combining five automation tools, Sightline ACE presents the configuration state of any infrastructure by automatically using the latest data from physical, logical and virtual data resources. Through auto-detection, ACE detects and helps manage real-time control and change across virtual environments across networks, servers and geographic locations.	http://sightlinesystems.com/products/sightline-ace/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
228	**Sightline Holdings Corp.**	**Enterprise Data Manager (EDM)**	EDM provides IT teams with a single, simple and yet powerful view into every part of a company's infrastructure from mainframes to the latest in Windows and Linux systems. EDM is scalable to the size of any business, capable of monitoring hundreds to thousands of infrastructure components with over 7,500 points of collected data.	http://sightlinesystems.com/products/enterprise-data-manager/
229	**Sightline Holdings Corp.**	**Power Agent**	Power Agents significantly increase the amount and fidelity of real-time performance and process data delivered to EDM. Every server, application and operating system generates data but Power Agents deliver IT teams access to data outside of the limited scope of scope of the manufacture data set.	http://sightlinesystems.com/products/power-agents/
230	**Solarwinds**	**DameWare Remote Support**	Comprehensive remote support software for end-user support and system troubleshooting.	http://www.solarwinds.com/products/
231	**Solarwinds**	**Enterprise Operations Console**	Unified visibility Into geographically distributed networks	http://www.solarwinds.com/products/
232	**Solarwinds**	**IP Address Manager**	Eliminate IP conflicts and save time managing DHCP, DNS and IP Addresses	http://www.solarwinds.com/products/
233	**Solarwinds**	**Log & Event Manager**	A SIEM that makes it easy to use logs for security, compliance, and troubleshooting	http://www.solarwinds.com/products/
234	**Solarwinds**	**Network Packet Analysis**	Network traffic analyzer and bandwidth monitoring software	http://www.solarwinds.com/products/
235	**Solarwinds**	**Network Performance Monitor**	Reduce network outages with affordable, easy-to-use network monitoring software	http://www.solarwinds.com/products/
236	**Solarwinds**	**Patch Manager**	Automated Patching and Vulnerability Management for Microsoft® and 3rd-party software	http://www.solarwinds.com/products/
237	**Solarwinds**	**SolarWinds Network Configuration Manager**	Automated Network Configuration & Change Management Software • Reduce configuration errors using standardized device configurations and deployment automation. • Improve network reliability using change monitoring, alerting, configuration backups and rollbacks. • Manage change using workflows to approve updates and safely delegate work to others. • Improve network security using IOS vulnerability scanning and NIST FISMA, DISA STIG, and DSS PCI compliance assessments.	http://www.solarwinds.com/network-configuration-manager.aspx
238	**Solarwinds**	**SolarWinds Server & Application Monitor**	Detailed application performance metrics for >200 applications •Exchange Monitoring - Mailbox database capacity, failover alerts, I/O •Monitoring IIS - IIS server performance, Websites & application pools •SQL Server Monitoring - Database status & capacity, Long-running queries and more •Support also included for Linux®, Active Directory®, Apache®, and Windows® Server monitoring	http://www.solarwinds.com/server-application-monitor.aspx
239	**Solarwinds**	**Storage Resource Monitor**	Multi-vendor storage performance and capacity monitoring	http://www.solarwinds.com/products/
240	**Solarwinds**	**User Device Tracker**	Always know when and where users and endpoint devices are connected to your network	http://www.solarwinds.com/products/
241	**Solarwinds**	**Web Help Desk**	Affordable & easy-to-use IT service desk for help desk ticketing and IT asset management.	http://www.solarwinds.com/products/
242	**Splunk**	**Splunk App for Enterprise Security**	The Splunk App for Enterprise Security is a next-generation security intelligence platform that addresses SIEM (Security Information and Event Management) use cases by providing pre-packaged dashboards, reports, incident response workflows, analytics, and correlations to quickly identify, investigate, and respond to internal and external threats. It also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.	http://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/splunk-app-for-enterprise-security
243	**Splunk**	**Splunk Enterprise**	Splunk Enterprise is a sloution that collects machine data from whereever it's generated, including physical, virtual and cloud environments. It enables users to search, monitor and analyze data from one place in real time. It offers out-of-the-box integration with traditional relational databases and new open source data stores drive more value from user data.	http://www.splunk.com/en_us/products/splunk-enterprise.html
244	**Symantec**	**Altiris**	The Symantec Endpoint Management software family of products powered by Altiris technology can help you drive down IT costs, improve efficiencies with comprehensive configuration management, take control and automate your IT infrastructure, and much more.	http://www.symantec.com/endpoint-management/
245	**Symantec**	**Control Compliance Suite**	Control Compliance Suite delivers business-aware security and risk visibility so that customers are effectively able to align priorities across security, IT operations, and compliance. It automates continuous assessments and delivers a unified view of security controls and vulnerabilities. With Control Compliance Suite, customers are able to harden the data center, prioritize security remediation, enable the secure migration to the software-defined data center, and support continuous assessments for Cyber Security and Continuous Monitoring.	http://www.symantec.com/control-compliance-suite/
246	**Symantec**	**Critical System Protection**	Critical System Protection is a lightweight security client designed to secure the Internet of Things (IoT) by protecting the endpoint and embedded devices. It offers manufacturers and asset owners of embedded systems robust signatureless, host-based protection in managed and unmanaged scenarios, without compromising device performance.	https://www.symantec.com/products/threat-protection/embedded-security

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
247	**Symantec**	**Data Center Security Server**	SYMC Data Center Security Server provides: * Agentless network-based threat detection and protection (Network IPS). * Operations Director delivers out-of-the-box security intelligence and automates policy-based security orchestration within the Symantec Data Center Security product family, enables application-centric security services, and seamlessly integrates with VMware * NSX to extend security policy orchestration to third party security tools. * Unified Management Console (UMC delivers a consistent management experience across Data Center Security products. * In-guest file quarantine and policy-based remediation. * Automate policy-based security provisioning and deliver always-on security with the best-of-breed security protection technology. * Optimize network and application performance of guests and hosts via agentless antimalware and agentless network IPS. * Improve network performance by having single definition updates. * Auto-deployment of virtual appliances enables the workloads to scale while minimizing any additional OpEx cost.	http://www.symantec.com/en/uk/data-center-security/
248	**Symantec**	**Data Insight**	Symantec Data Insight helps organizations improve unstructured data governance through actionable intelligence into data ownership, usage and access controls. Data Insight's reporting, analytics and visualization capabilities help drive efficiency and cost reduction across the data lifecycle as well as help drive improved protection of sensitive data and achieve compliance.	http://www.symantec.com/data-insight/
249	**Symantec**	**Data Loss Prevention (DLP)**	Symantec Data Loss Prevention (DLP) is a solution that addresses security, privacy and compliance issues so that users can take advantage of the cloud with control and visibility. It discovers, monitors and protects confidential data across cloud, mobile and on-premises environments.	http://www.symantec.com/data-loss-prevention/
250	**Symantec**	**Deepsight Intelligence**	Symantec DeepSight Intelligence collects, analyzes and delivers cyber-threat information through a customizable portal and datafeeds, enabling proactive defensive actions and improved incident response.	https://www.symantec.com/deepsight-products/
251	**Symantec**	**Encryption Management Server by PGP**	Encryption Management Server manages and automates security policies across Symantec's encryption solutions to defend sensitive data and avoid potential financial losses, legal ramifications, and brand damage resulting from a data breach. • Unified Administration Console – Eliminate the cost of maintaining multiple encryption consoles and minimize the risk of inconsistent security policies. • Symantec Protection Center - Integrate for multiple security product administration and reporting. • Logging, Monitoring, & Reporting – Reduce the time needed to audit activities around multiple encryption solutions. • Enterprise Integration – Fine tune policy assignment using optional enterprise directory integration, PKI, or organizational system management tools.	https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-management-server.pdf
252	**Symantec**	**Endpoint Protection**	Symantec Endpoint Protection 12.1 provides unrivaled security, blazing performance, and smarter management across both physical and virtual machines to protect against mass malware, targeted attacks and advanced persistent threats without compromising performance or business. •IPS & firewalls block malware as it travels over the network before arriving at your system •Unique intelligent security technologies derived from the largest global intelligence network •Support for Windows, Macs, and Linux across physical and virtual environments •Single, high-powered, seamless management console	http://www.symantec.com/pages.jsp?id=campaign-endpoint-protection&om_sem_cid=biz_sem_s1277722111
253	**Symantec**	**Identity: Access Manager (SAM)**	SAM is a next generation access control platform for the cloud that integrates Single Sign-On (SSO) with strong authentication (supporting Symantec Validation and ID Protection Service (VIP), Symantec Managed PKI Service (MPKI), and solutions that support integration through Radius), access control, and user management.	http://www.symantec.com/identity-access-manager/
254	**Symantec**	**Managed PKI (MPKI)**	Symantec Managed PKI (MPKI) is a soltuon for SSL cloud-based management consoles that provides centralized control and delegated administration of Symantec SSL and code-signing certificates. Extended Validation (EV) and premuim certificates include vulnerability assessments and malware scanning to assist in website protection.	http://www.symantec.com/ssl-certificates/managed-pki-ssl/
255	**Symantec**	**Mobility Suite**	Mobility offers any time, any place, and any device productivity appealing to both enterprises and employees. This same flexibility comes with the challenges of protecting corporate data on devices, separating personal and corporate information, managing diverse operating systems, and preventing devices and apps from becoming another attack vector.	https://www.symantec.com/products/threat-protection/endpoint-family/mobility-suite
256	**Symantec**	**Norton Secure Login (NSL)**	Symantec NSL is a cloud-based identity service that provides identity proofing, credential issuance, credential validation, attrribute validation, and single sign-on services.	https://www.symantec.com/content/en/us/about/media/repository/Norton-Secure-Login-Service-Description.
257	**Symantec**	**Protection Center Enterprise**	Symantec Protection Center Enterprise 3.0 (SPC Enterprise) is a powerful data collection and analytics platform. Leveraging this platform, you can communicate the impact of threats and IT risks in business terms. It lets you collect data from multiple security solutions, compute an aggregate business risk score, generate dashboards, and report and automate key processes using a workflow.	https://support.symantec.com/en_US/article.HOWTO82748.html
258	**Symantec**	**Risk Automation Suite**	SRAS automates and orchestrates enterprise IT security and risk management.	http://www.symantec.com/connect/forums/symantec-risk-automation-suite
259	**Symantec**	**Software Management For Clients And Servers Powered By Altiris Technology**	Symantec Client Management Suite automates time-consuming and redundant tasks for deploying, managing, patching, and securing desktops and laptops so organizations can reduce the cost and effort of managing Windows, Mac, Linux, and virtual desktop environments.	https://www.symantec.com/products/threat-protection/endpoint-management/client-management-suite

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
260	**Symantec**	**Validation and Identity Protection Service (VIP)**	Symantec Validation and ID Protection Service (VIP) is a cloud-based authentication service that enables enterprises to secure access to networks and applications as a unified solution providing both two-factor and risk-based token-less authentication based on open standards and can easily integrate into enterprise applications.	http://www.symantec.com/vip-authentication-service/
261	**Tanium, Inc.**	**Platform**	The Tanium Platform is a product that distributes management intellegence and data directly to the computing devices themselves. It is a peer-to-peer communications architecture that relies on sensors and packages to provide instant command and control through a web-based console for agile incident response, advanced endpoint protection, and continuous systems management.	https://www.tanium.com/products/
262	**TAPE**	**CyberForge Cauldron**	Cauldron visualizes potential attacks against the enterprise by building a network model using results from vulnerability scanners, asset management, firewall rules and other data sets as needed. Cauldron then predicts possible paths of cyber attack from its inputs to allow the enterprise to visualize cyber gaps, do “what if” analysis and validate mitigation methods before operational deployment. By aggregating “silo” data sets, the synergies created enable the security stakeholders to visually represent the impact of change (even a single element) on the entire cyber security eco-system	http://cyvisiontechnologies.com/section/Cauldron/9/
263	**Tenable**	**Log Correlation Engine**	Centralized Log Management	https://www.tenable.com/products/log-correlation-engine
264	**Tenable**	**Nessus Manager**	Nessus® Manager combines the powerful detection, scanning, and auditing features of Nessus, the world’s most widely deployed vulnerability scanner, with extensive vulnerability management and collaboration functions.	https://www.tenable.com/products/nessus/nessus-manager
265	**Tenable**	**Passive Vulnerability Scanner**	Tenable’s Passive Vulnerability Scanner™ (PVS™) eliminates network blind spots by continuously monitoring network traffic in real-time to discover active assets, identify cloud applications, and detect anomalous activity.	https://www.tenable.com/products/passive-vulnerability-scanner
266	**Tenable**	**Security Center Continuous View**	Tenable's SecurityCenter Continuous View (SecurityCenter CV) is a continuous network monitoring platform that provides braod coverage of the user environment, detection of vulnerabilities, misconfigurations, malware and real-time threats, advanced analytics, and Assurance Report Cards.	https://www.tenable.com/products/securitycenter/securitycenter-continuous-view
267	**Tenable**	**Tenable Series Appliance**	The Tenable Virtual Appliance replaces the Nessus VM Appliance and provides a preinstalled image of all Tenable applications in one easy to configure interface. The Tenable Virtual Appliance is available for Tenable customers and is provided for use with VMware Server, VMware Player and VMware ESX Server. Currently, Nessus and Security Center applications are available on the appliance with the Log Correlation Engine and Passive Vulnerability Scanner to be released soon.	https://www.tenable.com/products
268	**Trend Micro**	**Deep Security - Compliance Pack**	Trend Micro Cloud and Data Center Security solutions protect applications and data and prevent business disruptions, while helping to ensure regulatory compliance. Whether you are focused on securing physical or virtual environments, cloud instances, or web applications, Trend Micro provides the advanced server security you need for virtual, cloud, and physical servers via the Trend Micro™ Deep Security platform. •• Secures physical, virtual, and cloud environments with one comprehensive solution •• Provides the most complete set of security capabilities available from the global market share leader in server security •• Saves resources/reduces costs with automated policy and lifecycle management with optimized security •• Available as software or as-a-service with central management across hybrid environments	http://www.trendmicro.com/cloud-content/us/pdfs/sb_trend_micro_cloud_and_datacenter_security.pdf
269	**Tripwire**	**CCM for Network Devices**	Tripwire Configuration Compliance Manager automates auditing, change monitoring and compliance processes, delivering results. * Discovery and Audit: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches * Agentless Architecture: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful. * Compliance Automation: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.	http://www.tripwire.com/it-security-software/scm/ccm/
270	**Tripwire**	**CCM for Servers**	Tripwire Configuration Compliance Manager automates auditing, change monitoring and compliance processes, delivering results. * Discovery and Audit: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches * Agentless Architecture: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful. * Compliance Automation: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.	http://www.tripwire.com/it-security-software/scm/ccm/
271	**Tripwire**	**CCM for Single Purpose Devices**	Tripwire Configuration Compliance Manager automates auditing, change monitoring and compliance processes, delivering results. * Discovery and Audit: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches * Agentless Architecture: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful. * Compliance Automation: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.	http://www.tripwire.com/it-security-software/scm/ccm/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
272	**Tripwire**	**CCM for Workstations**	Tripwire Configuration Compliance Manager automates auditing, change monitoring and compliance processes, delivering results. * Discovery and Audit: Tripwire® Configuration Compliance Manager (CCM) utilizes active and passive scanning to discover and audit configurations. You receive highly detailed information on the configurations of your systems, applications, firewalls, routers and switches * Agentless Architecture: Tripwire CCM utilizes an agentless architecture, requiring no software to install on the monitored endpoints. You enjoy ease of management across the largest networks and highly cost-effective deployments. Simple and powerful. * Compliance Automation: Tripwire CCM automates continuous configuration and compliance assessment, making it easy for your policy engine to tune and modify custom policies. Maximize your resources with a process that supports your goals.	http://www.tripwire.com/it-security-software/scm/ccm/
273	**Tripwire**	**Device Profiler**	Tripwire's Device Profiler 5000 and 5050 are new, high performance vulnerability scanning appliances that discover and assess every IP address on a global network for over 100,000 security conditions. These models have been optimized for SCAP configuration compliance scanning and vulnerability scanning in the same infrastructure, dramatically reducing the total cost of ownership.	http://www.tripwire.com/register/device-profiler-datasheet/
274	**Tripwire**	**IP360**	TripWire IP360 Vulnerability Management solution will: * Discover What's On Your Network: Maintain security of your assets. Discover every device, software and application for a comprehensive view of your network. Build effective risk management and compliance processes. We're your first line of defense for threat security. * Fix What Matters Most: Find the most important vulnerabilities fast and address them immediately. Tripwire's unique vulnerability scoring allows you to prioritize vulnerabilities, so IT security teams can quickly and effectively reduce overall network risk	http://www.tripwire.com/it-security-software/enterprise-vulnerability-management/tripwire-ip360/
275	**Tripwire**	**Policy Manager**	Tripwire Enterprise Policy Manager: Continuously Monitor, Assess and Harden Your Systems. With a library of over 650 compliance policies for regulations and standards, and even policies for optimizing systems and services for availability and performance, Tripwire® Enterprise can help organizations successfully meet their cyber security and compliance needs.	http://www.tripwire.com/register/tripwire-enterprise-policy-manager-harden-your-systems-with-security-conf
276	**Tripwire**	**PureCloud Annual Subscription**	Tripwire PureCloud Enterprise provides an easy to deploy and cost-effective solution that discovers and assesses hard-to-reach areas of a network.	http://www.tripwire.com/it-security-software/enterprise-vulnerability-management/purecloud-enterprise/
277	**Tripwire**	**Suite360 Intelligence Hub**	Tripwire Suite360 Intelligence Hub improves accountability and effectiveness with automated risk reporting for all audiences * Measure Progress Over Time: Customizable dashboards provide at-a-glance information about the state of your organization's risk status and compliance initiatives. Integrate your security and configuration audit data into security portals, applications and business processes. * Promote Accountability: Improve accountability with reporting and analytics that measure enterprise-wide risk reduction within the context of your business. Trend data for hosts, networks, line of business and the organization as a whole. * Improve Operational Efficiency: Audience-specific reports address a wide range of enterprise audiences including executives, auditors, IT and security groups. Automate manual report generation and distribution so the right data reaches the right people more efficiently.	http://www.tripwire.com/it-security-software/security-analytics-reporting/tripwire-security-intelligence-hub/
278	**Tripwire**	**Tripwire Enterprise**	Tripwire Enterprise provides real-time threat detection, security automation and business context. * Real-time Change Intelligence: Get real-time threat detection and notification at the speed of change. Tripwire® Enterprise delivers change audit and threat detection with high precision, business context and insight for what to do about it * System Hardening and Compliance Enforcement: Tripwire Policy Manager delivers proactive configuration hardening based on compliance requirements, reduces audit preparation time and cost, and provides audit-ready reporting with evidence of compliance, remediation and exception management. * Security Automation and Remediation: Configuration errors need corrective measures. Tripwire Remediation Manager delivers automation and guidance for rapid repair of broken or security misconfigurations, and integrates with SIEMs, IT-GRC, workflow systems, change management systems and more.	http://www.tripwire.com/it-security-software/scm/tripwire-enterprise/
279	**Triumfant, Inc.**	**IT Management**	Triumfant solutions close the breach detection gap with rapid analysis and remediation. Our proprietary tools detect breaches in real-time, generate a comprehensive and actionable analysis within minutes of the attack, and perform situational remediation that stops the breach.	http://www.triumfant.com/triumfant-products-overview/
280	**Trustwave**	**AppDetectivePro**	AppDetectivePRO is a database and Big Data scanner that can immediately uncover configuration mistakes, identification and access control issues, missing patches, or any toxic combination of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service (DoS), or unauthorized modification of data held within data stores.	https://www.trustwave.com/Products/Database-Security/AppDetectivePRO/
281	**Trustwave**	**DbProtect**	DbProtect is a data security platform that uncovers database configuration mistakes, identification and access control issues, missing patches, or any toxic combination of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service (DoS), or unauthorized modification of data held within data stores (relational databases and Big Data). Through its multi-user/role-based access, distributed architecture, and enterprise-level analytics, DbProtect enables organizations to secure all of their relational databases and Big Data stores throughout their environment, on premise or in the cloud.	https://www.trustwave.com/Products/Database-Security/DbProtect/
282	**Trustwave**	**Intellitactics Security Manager**	Trustwave SIEM solutions help organizations of all sizes simplify management and operations, while delivering on big data intelligence security capabilities and interoperability demands of the toughest business, compliance and technical requirements.	https://www.trustwave.com/Products/SIEM/
283	**Trustwave**	**Log Management**	Simplified log management, compliance management and security coverage packaged in an appliance that is easy to install and manage. SIEM Log Management includes logging, correlation, dashboards and reporting, as well as ad-hoc analysis and forensic investigation capabilities and powerful searching, filtering and visual analysis.	https://www.trustwave.com/Products/SIEM/

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
284	**Trustwave**	**Network Access Control**	Embracing a bring-your-own-device (BYOD) culture can be a good thing – increased employee satisfaction and productivity with a lower total cost of ownership (TCO) for mobile devices. But BYOD also creates challenges, which can include managing non-standard, heterogeneous devices and personal and potentially rogue applications, as well as possibly introducing malware into the corporate network.	https://www.trustwave.com/Products/Network-Security-and-Access-Control/Network-Access-Control/
285	**Trustwave**	**Secure Web Gateway**	With Trustwave's award-winning and industry-leading Secure Web Gateway, organizations can detect malware on the fly without relying on signatures, gain zero-day protection against advanced threats and enable the safe and secure use of applications such as Facebook, Twitter and Gmail — all while	https://www.trustwave.com/Products/Content-Security/Secure-Web-Gateway/
286	**Trustwave**	**Web Application Firewall**	With our award-winning Web Application Firewall, you can continuously monitor your applications, instantly detect and prevent threats, mitigate the risk of data breaches, and address compliance requirements, including the PCI DSS (section 6.6).	https://www.trustwave.com/Products/Application-Security/Web-Application-Firewall/
287	**Varonis**	**Data Transport Engine**	Data Transport Engine makes it easy to migrate data cross-domain or cross-platform, all while keeping permissions intact and even making them better. Quarantine sensitive and regulated content, discover data to collect for legal hold, identify data to archive and delete, and optimize your existing platforms.	https://www.varonis.com/products/data-transport-engine/
288	**Varonis**	**DatAdvantage (DA)**	The Vaonis DatAdvantage software solution that aggregates user, permissions, data and access event information from directories and files serves. Analytics applied to the collected information can show detailed data use and determine rightful access based on business need.	http://www.varonis.com/products/datadvantage/
289	**Varonis**	**DataPrivilege (DP)**	The Varonis DataPrivilege automates data governance by providing a framework for users and data owners to be directly involved in access entitlement review and authorization workflows. AUTOMATED ENTITLEMENT REVIEWS • Data owners are provided scheduled entitlement reviews with recommendations for access removal (generated by DatAdvantage) • Reviews can be scheduled based on business policy, including multiple schedules for entitlement reviews ACCESS CONTROL WORKFLOW • Users can request access to data and group resources directly for themselves or requests can be made in bulk, with explanations and duration • Data owners and other stakeholders are automatically involved in authorization process • Users can create new folders that are automatically provisioned, permissioned correctly, and then managed by business data owners without requiring IT's assistance • Local account management enables stakeholders to delegate privileges, along with automated expiration of access • Permissions changes are carried out automatically once approval requirements are met • Permissions revocations are carried out automatically on their assigned expiration date	http://www.varonis.com/products/dataprivilege/
290	**Varonis**	**IDU Classification Framework**	Varonis quickly discovers sensitive content, shows you where it is exposed, and helps you lock it down (and keep it that way) without interrupting business.	https://www.varonis.com/products/data-classification-framework/
291	**Veracode**	**Discovery Scan**	Creates a catalog of all web applications — both known and unknown — via a massively parallel, auto-scaling cloud infrastructure that discovers tens of thousands of sites per week. Provides detailed intelligence about the application layer such as what types of application servers are running and whether authentication is required, unlike traditional network scanners that perform simple port scans to identify infrastructure components.	http://www.veracode.com/products/web-application-discovery/discovery
292	**Veracode**	**Dynamic MP Scan**	DynamicMP rapidly baselines your application risk by performing a broad, unauthenticated scan of all public-facing web applications, typically starting with a prioritized list identified by our Discovery technology.	http://www.veracode.com/products/web-application-discovery/dynamicmp
293	**Veracode**	**Mobile Application Reputation Service**	Veracode's App Reputation Service provides behavioral intelligence about mobile applications to help you determine which mobile apps violate enterprise policies for security and privacy. The App Reputation Service integrates with mobile device management (MDM) solutions to help you implement a secure BYOD program via automated app blacklisting.	http://www.veracode.com/products/mobile-application-security/reputation-service
294	**Veracode**	**Static Analysis/Dynamic Analysis**	Static code analysis, also commonly called "white-box" testing, looks at applications in non-runtime environment. This method of security testing has distinct advantages in that it can evaluate both web and non-web applications and through advanced modeling, can detect flaws in the software's inputs and outputs that cannot be seen through dynamic web scanning alone. In the past this technique required source code which is not only unpractical as source code often is unavailable but also insufficient.	http://www.veracode.com/products/static-analysis-sast/static-code-analysis

The purpose of the Continuous Diagnostics and Mitigation (CDM), Tools/Continuous Monitoring as a Service (CMaaS) Product Catalog is to provide CDM Program stakeholders and CMaaS customers with a comprehensive list of CDM security products on the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) CDM CMaaS Blanket Purchase Agreement (BPA). This guide serves as a mechanism to identify products that could be procured to meet specific capabilities. The information and data used to create the Tools/CMaaS Product Catalog includes the CMaaS BPA Awardee information, cross linked to product descriptions publicly available on the manufacturer's websites. Over the course of the CDM program, technology-based solutions will adapt with the evolving cyber-threat landscape and industry is expected to improve and develop new and increasingly robust solutions. As new CDM Program capabilities and Phases are executed, new products will be added to the BPA and this Tools/CMaaS Product Catalog will be updated accordingly.The Tools/CMaaS Product Catalog is not intended as an authoritative document for aligning a specific product with a specific capability requirement. It can, however, be used to support alignment and acquisition of specific products, support solution development based on capability requirements, and support Agency-specific technology roadmap development and refinement.

All product categorizations, descriptions and weblinks have been received from the manufacturers and are for reference only, subject to change at any time, and have not been modified or endorsed by GSA or DHS.

Item #	CDM Product Manufacturer	CDM Product Group	Manufacturer's Product Description from public website	Manufacturer's web link to more information
295	**Verdasys, Inc.**	**Digital Guardian**	The Digital Guardian platform provides: * Data Visibility and Control: If you don't have visibility into your organization's sensitive data, you can't protect it. Digital Guardian for Data Visibility and Control enables you to understand exactly where your organization's PII, PCI, PHI data is and how it's being used – without requiring pre- defined policies. It also delivers device control and encryption – all at affordable price. * Data Loss Prevention: Breaches are inevitable, losing data is not. Digital Guardian for Data Loss Prevention (DLP) gives you everything you need – the deepest visibility, the fine-grained control and the industry's broadest data loss protection coverage – to stop sensitive data from getting out of your organization. * Advanced Threat Protection: It takes a data-centric approach to advanced threat detection, incident response and prevention that ensures security travels with the data. Adding DG for Advanced Threat Protection gives you the only security solution that protects sensitive data regardless of the source of attack. * Savant Protection Application Whitelisting: Application whitelisting adds a critical layer of defense against evolving threats such as zero-day attacks that endpoint anti-malware frequently fail to detect. But most of today's whitelisting products are too difficult to deploy, time-consuming to manage, and reliant on a centralized database. Savant Protection is easy to deploy, transparent to existing operations and the most secure application whitelisting for Retail POS systems and industrial control systems.	https://digitalguardian.com/products/digital-guardian-platform
296	**VirtuStream**	**ViewTrust Software**	Viewtrust automates enterprise risk management and compliance, providing a 360° view of risk based on data consumed and analyzed from across the enterprise and its assets. Features include: Single View of Enterprise Risk * See a single view of all risk and threat data collected from point solutions (sensors) deployed in the environment. * Analyze enterprise risk on demand, by system, asset or sensor * Hierarchical drill down/roll up of risk score from enterprise level to department/mission level to asset and sensor level * Perform trend analysis to anticipate future risk state Comprehensive Risk and Compliance Management * View comprehensive enterprise dashboard for risk, compliance and cyber threat/impact analysis * Automated audit and compliance Automated Threat Remediation * Trigger automated workflows for risk mitigation and compliance control evaluation	http://www.virtustreamsecuritysolutions.com/viewtrust-software
297	**Vormetric**	**Data Security Manager**	The DSM enables your business to meet new security mandates, compliance requirements and risks across your organization at unprecedented efficiency by centralizing and simplifying the provisioning of encryption keys for all Vormetric products and many 3rd party devices. The result of centralizing control of such a breadth of data-at-rest security capabilities is low total cost of ownership, efficient deployment of new secure services, and most importantly, an increase in control and visibility of data across your organization.	http://www.vormetric.com/products/data-security-manager
298	**Xceedium, Inc.**	**Xsuite**	Xceedium Xsuite controls access, monitors, and records the activities of privileged users across hybrid cloud environments. Xsuite vaults and manages credentials, federates identities and protects systems regardless of where they're located.	http://www.xceedium.com/xsuite/xsuite-overview
299	**Xceedium, Inc.**	**Xsuite for AWS**	Xsuite is the first and only privileged identity management solution designed specifically to support the Amazon Web Services environment. Xsuite for Amazon Web Services adds a vital layer of protection to the AWS Management Console, the powerful administrative tool that enables users to create, configure, and control AWS infrastructure.	http://www.xceedium.com/xsuite/hybrid-cloud/xsuite-for-amazon-web-services
300	**Xceedium, Inc.**	**Xsuite for Vmware**	Access to vCenter Server provides privileged users with the ability to delete or modify virtual machines en masse, and make sweeping configuration and operational changes to the environment. Xsuite is fully integrated into the VMware management environment, offering full control of privileged users and comprehensive protection. And Xsuite manages privileged user access to both VMware guest systems and the underlying vCenter Server management environment. This unique capability helps ensure complete next generation privileged identity management across the entire hybrid cloud.	
301	**Xceedium, Inc.**	**Xsuite Mainframe**	http://www.xceedium.com/xsuite/hybrid-cloud/xsuite-for-vmware	http://www.xceedium.com/xsuite/hybrid-cloud/xsuite-for-vmware
302	**Xceedium, Inc.**	**Xsuite MSFT Office 365**	Xceedium's work with Microsoft ensures organizations can manage the risks posed by privileged users with administrative access to Microsoft online services such as Office 365®, Exchange, SharePoint®, and Lync®. Xsuite is the only privileged identity management solution delivering next-generation capabilities for the entire hybrid cloud, including cloud-based software as a service offerings like Microsoft's.	